# ePass OTP Authentication System White Paper

# Directory

# 1. Overview

The rapid growth of the Internet has fundamentally changed peoples lives, with increasing online services such as online-shopping, online-offices, online-banking, as well as e-commerce being implemented in different types of fields (financial, stock market, telecom, government etc), providing a diverse range of applications and great convenience. While there are enormous productivity benefits available from increased access, the security risks have also largely increased by using the traditional access methods of authentication through static user IDs and passwords only. Users are lagging behind development and relying on single static passwords, which are wholly inadequate to the access requirements for authentication. Most have come to realize the need for strong authentication, as the static password carries all of the risks normally associated with weak authentication, including password theft, leaving sensitive applications and various types of data vulnerable to mischief.

Facing this - how to avoid security disadvantages and improve our access control?

The ePass OTP Authentication System allows you to create strong event-based two factor authentication security by using a dynamically generated one-time-password, also allowing you to combine this with your existing static password seamlessly.

# 2. Principle of Authentication

The ePass OTP Authentication System provides strict access control, based on strong two factor authentication. “Two-factor Authentication” is a more secure method. Just as the name implies, it requires two separate security elements, something you know (like the user password) and something you do not know (random one-time-password). ePass OTP Authentication System helps the user to store basic authentication information if user failed to provide the first factor, and meantime, generate the dynamic authentication identifier combined with the first one to implement the strong two-factor authentication.

Once the user has been inputted and registered into the ePass OTP Authentication System, he/she will be issued with a corresponding OTP token with their personal information recorded in the database. When logging in or securely accessing a resource, the user will depress the token’s button to generate a random and unrepeatable one-time-password, which they will then append to their original static user password during the user login phase.

Process flow and authentication architecture of the ePass OTP Authentication System:

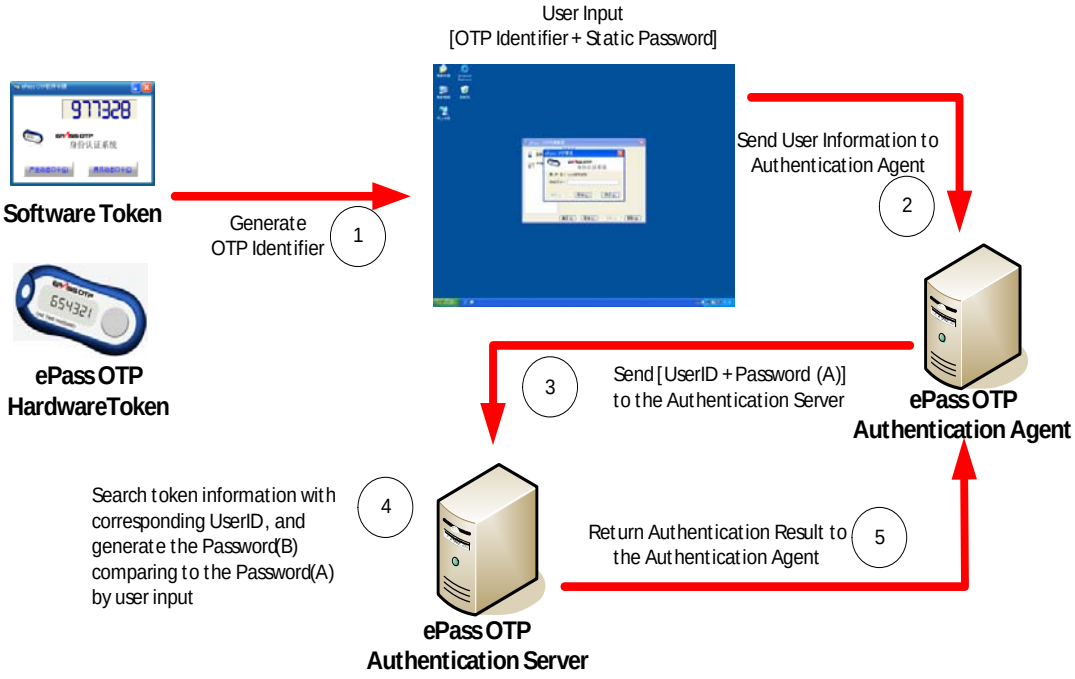


Figure 1 Process Flow of the ePass OTP Authentication System

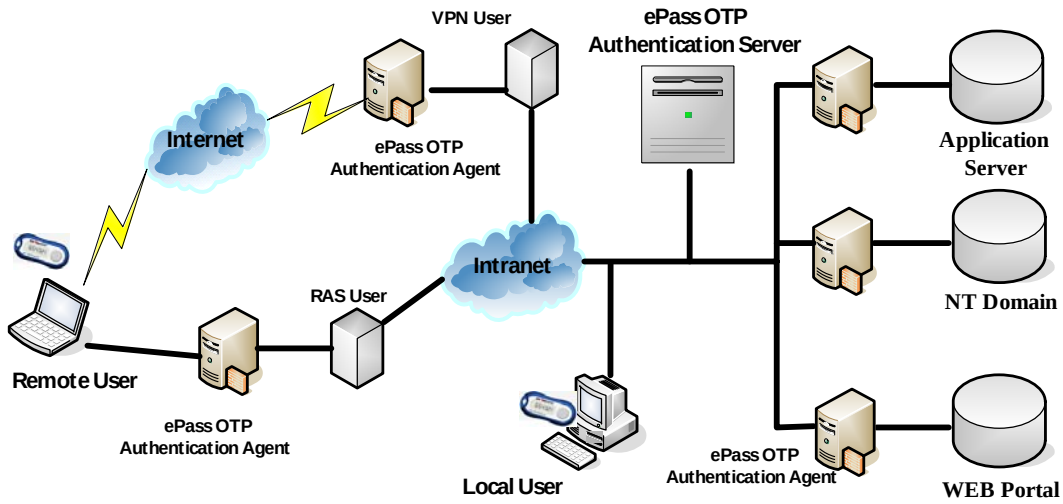


Figure 2 Authentication Architecture of the ePass OTP Authentication System

# 3. ePass OTP Authentication System

The ePass OTP Authentication System involves three components; the ePass OTP token, ePass OTP Authentication Agent and ePass OTP Authentication Server.

ePass OTP token:
In generating the one-time-password, each time when the user depresses the physical button on the token, a random algorithm-based password is generated dynamically. This dynamically generated password is absolutely necessary, along with the username and static password, to access resources protected by the ePass OTP Authentication System. In addition, the dynamic password is generated randomly, and only one time, to effectively avoid forecasting and tracking, thus dramatically increasing access security and greatly reducing the risk of password theft. Additionally, it simplifies the task to frequently change the password and makes it unnecessary to remember complex passwords, offering maximum flexibility for user authentication.

ePass OTP Authentication Server:
The ePass OTP Authentication Server runs under the network environment and consists of the following three parts:

- Database: used to centralize and store user information, token information and all related information
- Authentication Server Engine: processes authentication based on data transferred from the authentication agent
- Management Program: provides a graphical user interface (GUI) for the administrator to manage the system

ePass OTP Authentication System:
Provides / supports many types of authentication agents:

- Supports various VPN and Remote Accessing environments
- Supports various RADIUS-standard network devices from mainstream suppliers; eg. Cisco, Huawei, Juniper, 3Com etc.
- Supports Local-site Secure Logon and Domain Logon Authentication of Windows XP/NT/2000/2003 Server
- Supports Logon Authentication of various application systems; eg. Apache, IIS etc.

# 4. Features

- Open Architecture supports multi-OS, such as Windows NT/2000/XP/2003 Server/Vista
- Multiple Databases supported, such as Oracle, MySQL, SQLServer, PostgreSQL, MSDE, Access etc.
- Encrypt-protection of token Seed Code and anti-exhaustion protection of token password. In particular, the ePass OTP token will be locked if authentication fails four-consecutive-times
- Strong two-factor authentication supported, dynamically generated one-time-password, dramatically increase access security
- Compatible with both standard and extensible RADIUS protocol, allowing for user remote dial-in accessing
- All user-key-data communications (like user passwords) are securely encrypted during transfers of information from the Agent Server to the Authentication Server.
- Multiple Web Services supported, such as IIS and Apache, allowing for special access control to specific web pages
- Seamlessly integrates with other authentication services, allowing for deployment without any change to the current system
- No restriction to client-side application environment - due to the offline token usage. Such environments as PC machines, telephone entrust systems, ATM machines, as well as POS machine are all available to use secure ePass OTP tokens
- One-way and straightforward authentication process, preventing illegal accessing from unauthorized users effectively
- Easy to manage and flexible to use
- High concurrent-event supported - continuously taking into account optimization
- based on mature technologies applied, to make sure maximum number of run-time concurrent authentications
- Load balance implementation to support priority processing authentication requests from multiple servers

# 5. Technical Guideline

- Dynamically generated OTP: 6-decimal-digit, and event-based password renewing
- System Users: the maximum number of concurrent authentications is greater than 250 per second, with satisfaction of mass user application in distributed systems
- Data is self-destructed once token is physically broken
- OTP Token Operating Temperature: -20℃ to 70℃ water-resistance (IP54), static-resistance, electromagnetic-resistance, quake-resistance
- Battery Lifespan: 5 years
- Qualification: Compliant with CE and FCC standards
- Communication Protocol Supported: TCP/IP, RADIUS

# 6. Typical Application

- IIS Secure Authentication: applied in online stock-exchanging, online banking, online education and other business ecommerce web services
- OA Secure Authentication: applied in all kinds of business official automation systems
- Call-Center Secure Authentication: applied in calling entrust centers of stock market, calling service centers of bank systems, as well as special calling service centers etc.
- Dial-in Network Accessing Secure Authentication: applied in mobile office, remote network administration, dial-in backup, banking, stockmarket, government, and public security systems
- NT Domain Secure Authentication: applied in logon authentication systems for both user and local areas of business and government-levels
- TELNET/FTP Secure Authentication: applied in remote network administration for online stock-exchanging, online banking, online education and other business e-commerce web services
- APACHE Secure Authentication: applied in online stock-exchanging, online banking, online educating and other business e-commerce web services
- ERP Secure Authentication: applied in business management systems of mid-level above
- Network Equipment Secure Authentication: applied in logon authentication systems for both user and business local area networks
- VPN Secure Authentication: applied in logon authentication systems for both user and business local area networks

RS-Computer Vertriebs GmbH & Co. KG
Your Trusted Security Partner
Frankenring 9 * 30855 Langenhagen * Germany
e-mail: info@rs-computer.com
Web: www.rs-computer.com
Voice: +49 511 67 48 50
Fax: +49 511 67 48 525