

Time-Based vs Event-Based Two-Factor Authentication

The difference between time and event-based tokens

Time-Based vs. Event-Based Tokens

Deciding on a Token Type

Before deciding on an authentication solution for your organization, it is important to know the difference between Time-based tokens and Event-based tokens.

Some things to consider are:

- Level of Security
- Ease of Use
- Total Cost of Ownership
- Flexibility

Time-Based tokens

Time-based tokens were developed to provide simplicity and compatibility. While this may have been accomplished, several issues were introduced (e.g. user inconvenience, security weakness):

- Each token and server requires a clock. Every 30 or 60 seconds a new 'response' is presented. The current time (input value) is encrypted using the token's secret key and results in an encrypted number which becomes the one-time password. The problem with this is that two clocks rarely have the same time. Throughout the token's lifespan, the time drifts to a substantial difference between the token and the server.
- To work around this problem, a 'window' must be set on the server to allow passwords to be accepted +/- 3 minutes. Therefore, if the token is set to increment at 30 second intervals, 13 password values would be accepted as correct.

- This would allow a 'shoulder surfer' or a 'network sniffer' to log in with one of the other valid passwords.
- If a user mistypes their one-time password during their login and needs to re-enter it, they must wait 30 or 60 seconds for the next password to appear.
- If an organization has 10,000 users, and if each month they need to wait an average of 2 times for a password to appear and enter the correct code in the time frame, the annual cost is \$75,000.00 – over \$12,000.00/month.
- Tokens continuously display valid pass codes, which could be seen by anyone around.
- If an organization has a policy not to share their 'secret key', they cannot purchase a time-based solution.
- Time-based tokens are pre-initialized by the manufacturer. Therefore, the manufacturer has a copy of each secret key for every token ever sold.
- Lifespan of time-based tokens is between 24 and 60 months, at which time the token stops working. The organization must ensure that each employee has a replacement token prior to this happening (which entails purchasing another token and deploying it – two costs that will be repeated every 2-5 years).

Event-Based Tokens by CRYPTOCARD

Event-based tokens were developed to provide robust, easy-to-use yet highly secure tokens with none of the disadvantages and security problems associated with Time-based tokens:

- No internal clock is required, so no time-drifting occurs.
- Well-understood, publishable crypto algorithms of known strength that have been subjected to and withstood expert scrutiny (DES, 3DES, AES 128-bit, 192-bit, 256-bit).
- Very rarely does manual resynchronization have to take place, as the token does not automatically increment to the next response without user intervention.
- All software/smart card/USB tokens are PIN protected, which means the one-time password will not be displayed until the user enters the PIN (that only they know) into the token.
- Hardware tokens can be programmed to require the entry of a PIN into the token to 'activate' it. Only then will the token display a one-time password. Hardware tokens can also be configured with server-side PIN, which requires the user to enter the PIN, appended by the one-time password – in order to be authenticated.
- Tokens are initialized by the end-user, so the 'secret key' resides only with the organization.
- As there is no internal clock, tokens do not expire. Every 4-6 years, the watch batteries in the hardware tokens will have to be replaced, which the end-user can do. Therefore, there is no additional purchase/deployment costs/inconveniences which are associated with time based tokens.

Key Features of CRYPTOCARD's Event-Based Tokens:

- Eliminates the use of static passwords and replaces them with one-time passwords
- Secure remote and internal network access with two-factor authentication
- Compatible with leading remote access servers, VPNs, firewalls, Web servers, and Wireless access points
- CRYPTOCARD tokens are used by thousands of companies in over 70 countries
- CRYPTOCARD tokens leverage security technology partnerships with, and testing against, over 250 leading vendors, including Microsoft, Apache, Apple, Cisco Systems, Citrix Systems, Check Point and Juniper Networks

Summary

When your organization has made the decision to purchase an authentication system, the success of the project will depend on how well users accept their authentication devices, and how easy it is for administrators to deploy the tokens, educate the users and support the entire system.

Ensure that the overall authentication suite (software and tokens) provides you with the flexibility, performance and reliability that you are looking for.

About CRYPTOCard

Established in 1989, CRYPTOCard provides cost-effective Secure Password Technology™ to leading enterprises worldwide in the government, technology, aerospace, financial, telecommunications, and healthcare sectors. Winner of the Best of Show, award at Macworld 2004, and SC Magazine's Best Buy Award for 2005, CRYPTOCard positively authenticates a user's identity by coupling something in the user's possession (a Smart Card, hardware token, or software token), with something the user knows (their PIN), and provides centralized authentication for all physical and network access regardless of network infrastructure or user location. CRYPTOCard's partners include Citrix (Nasdaq: CTXS), Apple (Nasdaq: AAPL), Cisco (Nasdaq: CSCO), Check Point (Nasdaq: CHKP), Entrust (Nasdaq: ENTU), Oracle (Nasdaq: ORCL), Sun Microsystems (Nasdaq: SUNW), and Macromedia (Nasdaq: MACR). For additional information on CRYPTOCard, please visit www.cryptocard.com.

CRYPTOCard North America

340 March Road
Suite 600
Ottawa, Ontario
K2K 2E4 Canada

Toll Free: 800-307-7042
Tel: +1-613-599-2441
Fax: +1-613-599-2442
E-mail: info@cryptocard.com
www.cryptocard.com

CRYPTOCard Europe

Eden Park, Ham Green
Bristol BS20 0EB,
United Kingdom

Tel: +44 870 7077 700
Fax: +44 870 7077 711
E-mail: info@cryptocard.com
www.cryptocard.com

CRYPTOCard and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCard Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.
© 2006 CRYPTOCard Inc.
All rights reserved.

20061023