

---

# Universal Authenticated Logon

## A White Paper

## Table of Contents

1.	OVERVIEW .....	1
2.	THE PROBLEM WITH PASSWORDS .....	1
3.	CHARACTERISTICS OF AN EFFECTIVE PASSWORD MANAGEMENT SYSTEM .....	2
3.1	EASE OF USE.....	2
3.2	BUY TIME.....	3
3.3	BALANCED RISK .....	3
3.4	CONSISTENT LOGON EXPERIENCE .....	4
4.	“ATM” FOR THE MASSES .....	4
4.1	ONE-TIME PASSWORD (OTP) TOKENS REVISITED.....	4
4.2	SO WHY HAVE OTP TOKENS FAILED (SO FAR) .....	4
4.3	EVENT BASED OTP TOKENS .....	6
5.	INTRODUCING EUS-BASED TOKENS .....	6
6.	CONCLUSION .....	8

---

CRYPTOCARD Corporation, Suite 304, 300 March Road, Ottawa, Ontario. K2K 2E2, Canada

(613) 599-2441

## 1. Overview

---

All organizations are faced with the problem of protecting their digital assets and to that end apply a wide range of policies, technologies and training resources, at significant costs in both time and money. While it's difficult to argue against the wisdom of compartmentalization and layering, the final outcome is almost inevitably more complexity and less flexibility for IT staff as well as end-users.

The reality is that virtually all computer systems are protected from humans through the use of passwords. This includes the applications and resources they access as well as the security systems that are intended to protect them.

The purpose of this paper is to offer ideas that can be applied to any network, to largely remove humans from the security equation – thereby insulating them (and the systems requiring protection) from the deficiencies associated with passwords. Security is improved when sophisticated authentication techniques are applied before access to electronic resources is permitted. The latest advance in One-Time-Password technology is introduced, EUS-based tokens, which bring the concept of uniform and universal authenticated logon within reach.

## 2. The problem with Passwords

---

Passwords are not going away any time soon. In terms of the computer age, passwords originated as both an effective and convenient way to protect assets that were most often already protected through limited or controlled physical access. All of these conditions have radically changed in recent years except one – people.

What was once convenient and effective is now a nightmare because pervasive electronic access has replaced restricted physical access; one password has become many passwords; one environment has become a myriad of operating systems, applications and content delivery systems. People can't keep up. To compensate, end-users deal with passwords by writing them down, sticking them to their computers, sharing them or never changing them.

On top of this we ask end-users to manage their passwords. And why should end-users manage passwords? After all, it's not their assets that are being protected. Yet, end-users are quite capable of effectively managing and protecting passwords. If you don't believe it, ask a colleague to tell you their ATM bank card PIN number. They won't – even though your knowledge of the PIN is irrelevant unless they also give you their ATM bank card. Try explaining this rationale and ask for the PIN again. They still won't give it to you, quite simply, because they perceive the risk as being both high and personal.

So why are passwords so ineffective? Consider the problem again. It's not passwords that are bad – it's too many passwords that are bad. It's not that passwords are ineffective – it's weak, static passwords that are ineffective. It's not the vast array of applications that cause the problem – it's the lack of a consistent authentication methodology across all applications. It's not the cost of passwords – it's the cost of managing passwords (caused by the above). And passwords do have a huge advantage. They can be used in almost any situation or environment because they are generally not dependent on the presence of some underlying technology.

A great deal of effort has gone into the development and marketing of technologies to replace password systems, generally with disappointing results. The problem of course is that most of the alternatives are too technically complex to implement and manage, too costly, too rigid, or simply mask the problem.

For example, while PKI technology offers much more than an alternative to passwords, it has failed to capture the market because it is too complex to implement, a bear to manage and incredibly expensive. Paradoxically, PKI systems generally depend on static passwords to protect the various elements that make up the system – PKI simply builds, and applies a layer of complexity and cost, on top of static passwords.

Alternatives such as Single Sign-On (SSO) systems can alleviate the burden of password management from the end-user but do so by shifting it to the IT department. While there are variations on the theme, SSO systems essentially 'playback' a previously recorded, valid password. They do this through systems as basic as keystroke logging to more sophisticated 'scrap' recognition. Logon transparency often requires applications to be opened up so that the SSO system can hook directly to it. And when all is said and done, the myriad of static passwords still exist and are transmitted across the network.

The biggest step towards network security a corporation can take is to NOT let users be in possession of their own passwords.

### 3. Characteristics of an effective Password Management System

---

#### 3.1 Ease of Use

For a password management system to be effective it must be applicable across the entire end-user population, regardless of technical savvy, location or environment. To that end probably the most successful implementation of such a system is the "ATM" card used by financial institutions. It succeeds with virtually any end-user because it is a consistent and universal logon method that is simple to use, and it insulates the user from the complexity

of the security process. Who doesn't use their card, with their PIN, to access their money? In terms of the end-user population, is there one that is any more diverse? Probably not.

But the ATM card's success is derived from a unique set of circumstances that few organizations can duplicate. By controlling the applications and the network, financial institutions limit interoperability issues and largely eliminate the concerns related to transmitting static logon information across the network. They also have the advantage of risk imbalance – end-users will protect their card and PIN because they know these factors are protecting their personal assets.

### **3.2 Buy Time**

The system must be sufficiently complex to dissuade casual attackers/abusers and be capable of delaying a professional attack long enough to permit detection, in order to mount an appropriate response. In this sense the ATM card is also effective, but not primarily because of the underlying technology. ATM cards are effective because the institution controls the network from end-to-end, therefore the transmission of data including static security information can be secured – an enviable position that few organizations can duplicate. A controlled network permits the use of static information. Two-factor authentication is based on something the end-user has (the card) plus something they know (the PIN) thereby providing the 'system' confidence that the end-user is whom they claim to be.

Attacks on ATM cards have generally succeeded not because of a fault with the end-user, but rather by taking control of the process. Consider the attacks performed at gas bars or convenience stores. An ATM card is run through a terminal that the bank does not control, capturing both the card data and the end-user PIN. The apparent transmission or card failure is rectified when the card is run through a second 'real' terminal. The static nature of the information captured during the first transaction allows the attacker to steal the identity of the end-user. While the approaches vary in other types of attacks, ultimately they all depend on taking control of the transaction. Most importantly, they do not succeed because of a failure of the end-user.

### **3.3 Balanced Risk**

Security would be much easier to implement with balanced risk. The ATM approach succeeds because of a high-risk imbalance, perceived or real. It's this imbalance that causes the end-user to be so protective of the card and PIN. Yet in most organizations, the risk imbalance is skewed against the organization. At a minimum, an organization cannot and should not rely on the end-user to practice good security.

### 3.4 Consistent Logon Experience

Much like the ATM approach, the ideal solution requires an end-user to go through the same consistent, familiar, easy steps whenever accessing a protected system. The ATM card approach succeeds because it provides a consistent and familiar experience that requires the end-user to do two things at each logon: insert their card and enter their PIN. End-users are insulated from the underlying security system and any technical complexity.

## 4. "ATM" for the Masses

---

In most organizations an "ATM-like" experience would be a welcome relief to end-users and IT departments alike. However several improvements are required to make this approach effective and secure for use in most organizations.

### 4.1 One-Time-Password (OTP) tokens revisited

OTP token-based authentication is a technology that's been around for more than 20 years, predating pervasive distributed computing in most organizations. From a security point of view it is a technology that continues to be very successful because it solves the problem of who controls the network by combining two-factor authentication with one-time passwords. As with the ATM card, two-factors (card and PIN) provide a very high degree of confidence that end-user "Bob" is really "Bob". Whereas ATM cards fail on public, or uncontrolled, networks and equipment because of the static nature of the card - OTP's succeed by ensuring that the password generated by the card is unique, unpredictable and different for every transaction. While ATM cards are useful only on specific, controlled access points, tokens can be used anywhere a logon is permitted.

### 4.2 So why have OTP tokens failed (so far)

Despite claims of "most trusted" and so on by some manufacturers, token-based authentication has failed to replace the bulk of static password protected systems primarily because of cost, manageability and transparency.

The first commercial OTP systems were based on the Challenge-Response methodology. While extremely reliable and effective, Challenge-Response tokens met with a degree of resistance because they required the end-user to key a numerical "challenge" into the token and then key the resulting password "response" into the application.

In response to the resistance, time-based tokens were introduced. They provided an ease-of-use improvement on challenge-response by removing the need for the end-user to key a challenge into the token. By relying on time as the "challenge" the token is able to

automatically generate passwords. Of course, in practice, much of this ease-of-use was offset by time-synchronization problems.

Time-based tokens introduced two new problems as well, though one of these has only recently been recognized. The first issue is primarily cost. In part due to the demands of the technology and in part marketing opportunism, time-based tokens must be regularly replaced and redistributed. On average, the costs to support this type of program are prohibitive for most organizations. And because the technology is only reliable on dedicated hardware tokens, there is little opportunity to provide ATM card-like transparency. The end-user must always interact with the token.

The second issue has only come to light as organizations move towards applying a consistent authentication methodology, regardless of the location of the user, in the network. Much like the ATM approach, the two-factor authentication mechanism used by time-based tokens relies on the security of the network because one of the factors (the PIN) is broadcast across it. Clearly this is a poor strategy if a uniform, secure and universally applicable end-user logon experience is to be achieved. Introduced when remote access was predominantly manifested by dial-up access, broadcasting one of the time-based token factors, the PIN, across the network presented little risk.

Organizations invest so heavily in security products precisely because control of the network is so difficult to achieve. This gives rise to significant concerns where time-based tokens are to be used on shared and 'presumed secure' networks such as the internal LAN – because the PINs may be visible to all network users. Single factor authentication is the result.

In other words, time-based tokens are only two-factor based on something you have, "the token" and something the network is, "relatively secure".

The reality is slightly worse. Time-based tokens are always delivered "pre-programmed". Consequently, the organization essentially shares the other factor "something you have" with the supplier. This questionable two-factor arrangement has at times been referred to as something shared (organization /supplier) and something everybody knows.

Recall that end-users are very protective of their PINs when it's their assets that are being protected. Clearly they recognize their risk. It is unlikely that end-users would embrace a solution for protecting their assets if it relies on publishing their PIN - yet organizations often don't make the same distinction. This is most likely the result of a compromise between security and ease-of-use. Still, time-based tokens are better than static passwords.

### 4.3 Event Based OTP Tokens

The recent introduction of event-based OTP tokens provides the advantages of time-based tokens and eliminates their associated disadvantages. Event-based tokens use encryption to automatically generate a new, random challenge - which in turn is processed to produce a new, random password for each logon. The result is the same ease-of-use found in time-based tokens.

Time is not a factor in this technique, therefore event-based tokens do not suffer from the chronic time-synchronization problems of their time-based predecessors. Event-based tokens are not pre-programmed by the supplier. With event-based tokens, the "something you have" is truly "something only you have".

The other key shortcoming of time-based tokens, the broadcasted PIN, is also remedied by event-based tokens that require the PIN to be entered into the token to activate it. This approach ensures that the PIN remains a secret ("something only you know"). As a consequence, event-based tokens do not present the same risks associated with the misplacement or mishandling of time-based tokens. Furthermore, event-based tokens permit 'PIN-protection' against tampering in the event they are lost, misplaced, or stolen - after a (user selectable) number of incorrect PIN attempts, the token logic erases itself (analogous to a snake-eating-its-own-tail).

Event-based tokens have one other key advantage; they do not constantly display passwords. Not only does this extend the in-service life of the token (which results in a per user cost typically 1/2 that of time-based tokens), it also means that they are suitable for use in software and smart card formats.

Event-based tokens represent a substantial step forward in OTP technology. The introduction of a truly secret PIN, that replaces a broadcast PIN, permits this token type to be used securely and reliably regardless of the location of the user. This means that IT departments no longer need to distinguish between internal logons and external logons. Instead, using event-based OTP tokens, they can largely eliminate the issue of static password management and provide an end-user with a single logon methodology.

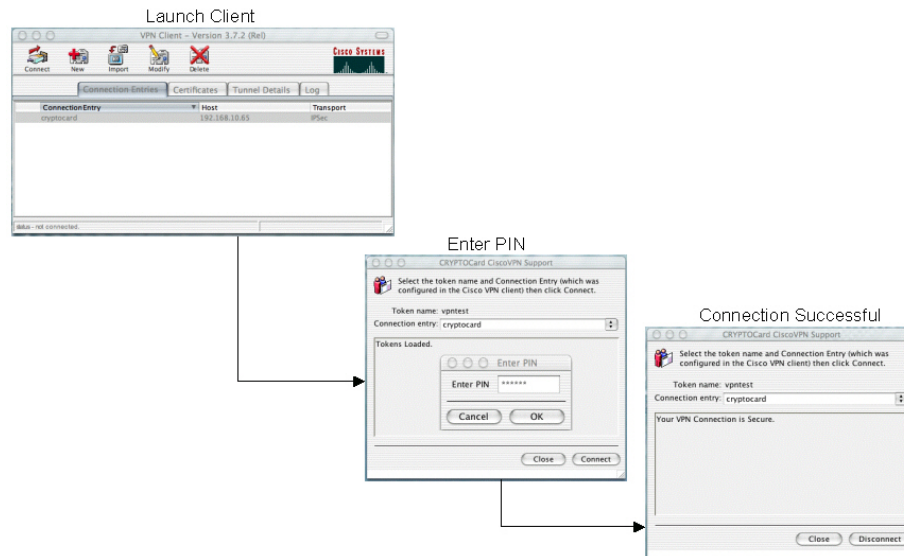
Event based tokens come much closer to the ATM card experience.

## 5. Introducing EUS-based (End-User Service) tokens

---

EUS-based tokens (End-User Service) are the most recent advance in OTP token adaptation. EUS-based tokens provide all of the functionality of event-based tokens with several advantages. EUS-based tokens install as a service on the end-user machine and can be called by a wide range of applications. During logon, the application requests a password

directly from the EUS. The EUS reacts by prompting the end-user for the PIN. If the PIN is correct, the EUS token generates a single OTP, completing the logon without further end-user intervention. In doing so, the EUS achieves what no other OTP token does – the true ATM card experience.



**Figure 1 A typical EUS authenticated Logon**

EUS-based tokens present a common user interface for all logons. They also provide a common application level interface, which allows all EUS-based tokens to be integrated with 3<sup>rd</sup> party applications, such as VPN clients, producing an automated and near transparent end-user logon experience. The same functionality can be enabled for web servers, portals, LAN authentication and a growing list of applications. EUS tokens can be integrated in custom or legacy applications using readily available APIs. Once integrated, the application will be compatible with any EUS-based token type. The result is a common logon experience for the end-user for both internal and external access to the network.

The actual token itself can reside either on the end-user machine or on an external device such as a smart-card. In this way EUS-based tokens achieve portability between machines, where necessary, desirable, or appropriate. They also provide strong physical and software protection of the token against tampering. Yet, they preserve a consistent, familiar logon experience regardless of platform, environment or location. The application of EUS technology to smart-cards yields additional functionality and flexibility. The smart-card becomes more than a logon card. It can take on a multi-function role that can include building access, PKI certificate storage, photo ID badge, loyalty card and much more.

EUS-based tokens introduce several key management features as well. They support electronic distribution and revocation making them substantially more convenient and cost

effective to distribute than traditional dedicated hardware tokens. They are orders of magnitude less expensive and less complex than PKI or SSO solutions.

## 6. Conclusion

---

While it is likely that no single password technology will satisfy all requirements, all of the time, universal authenticated logon can be a reality for most organizations by applying EUS-based OTP tokens.

Consider the outcome of an EUS implementation: the security of true two-factor authentication combined with OTP; a consistent and simple ATM-like logon, everywhere, all the time; "out-of-the-box" support by virtually all network access devices and many applications; electronic distribution and revocation; no dramatic change to, or investment in, infrastructure.

And then there are the people - end-users can be insulated from the diversity and complexity of their computing environment. Digital and intellectual property assets can be protected from the infrastructure level through the application level. Finally, IT departments have fewer password-related threats, help-desk, support, management, enforcement, and deployment issues to contend with - thereby saving themselves (and their organizations) considerable time, headaches, frustration and money while significantly improving the overall level of network security and accessibility.