» Two-factor authentication «

Considerations for selection of a two-factor authentication system. Written by Duncan de Borde, Siemens Insight Consulting

In order to provide trustworthy remote access to business services, secure authentication systems need to be used. Basic username and password authentication is no longer considered secure enough to protect a companies computer based assets. Any organisation looking into the introduction of a secure authentication system will be faced with a variety of complex choices. Selection of inappropriate technology, or failure to consider all the needs of the authentication system during the decision-making process, can prove an expensive mistake.

It is important to ensure that the system as a whole, not just the choice of technology, continues to meet the needs of the business, its users, business partners and possibly online customers, both in the short and long terms.

If the correct decisions are made early in the project, there is a significantly greater chance that the inheritance will be an authentication system that can reduce risk for the business, open up further opportunities to enhance on-line capabilities, and can remain in operation for a longer period, continuing to provide return-on-investment.

Wherever a high level of risk is identified with the danger of invalid users gaining access to systems, the use of some form of authentication stronger than a simple username and password may need to be considered. Traditionally the use of "strong authentication" has been largely associated with closed communities, such as authenticating employee access to corporate networks, though increasingly this is becoming a risk that needs to be addressed for the wider on-line community, e.g. in the case of online banking. As boundaries between businesses become more blurred, with customers or suppliers being allowed access to corporate systems, this will also become a consideration for business to business relationships.

This article highlights some of the issues that may need to be considered when selecting the right authentication solution for the business problem, which should not only include the choice of authentication technology, but also consider the supporting systems, processes and how they will fit in with the business model.

Authentication factors
Authentication establishes a level of confidence that the identification provided (e.g. username) is authentic. Most authentication methods today rely on one or more of the following factors:

- Something you know
- Something you have
- Something you are.

A password is an example of "something you know". To establish a level of trust it must be something that ONLY the user knows. Passwords that often get shared or written down can be intercepted (e.g. over the network, or by key loggers) or weak passwords can be cracked.

Dependent on the level of risk identified, this form of authentication on its own may no longer be sufficient. More innovative use of the "something you know" factor, such as selection of password/PIN characters from a drop-down list or image selection may help to address part of the problem, such as key logging, but still rely on the same basic principle.

The "something you have" factor requires the user to be in possession of something. This "something" is usually referred to as a token. A token is typically, but not necessarily, a hardware device that has been issued to the user for the purposes of authentication. There are various forms of token which are described later.

The important attributes are that the token can be authenticated by the system and uniquely associated with the user. The process of authenticating a token should use some form of "strong authentication" that is less easily compromised than a simple password, i.e. using some form of cryptographic process.

The "something you are" factor refers to some form of biometric authentication, based on a measurement of some personal characteristics (which may or may not be physical). It is important here to understand the difference between the use of biometrics for authentication and identification, which may impose different requirements on the process (biometric identification can spot a known person in a crowd, whereas biometric identification validates a claimed identity). Multiple forms of biometric authentication are available, all of which may enhance the level of confidence in the authentication process. At present the applicability of biometric authentication to the on-line community may be limited, with it being better suited to a more closed community. Not all biometric authentication methods require dedicated or expensive hardware; however all do require some initial measurement to be taken during registration.

Whilst biometrics will have a part to play in some situations, in most cases where the desire is to increase the level of trust in the authentication process over passwords, the use of a token is often the most appropriate choice. It is important to consider that "something you have" also has its own inherent weakness - it can be stolen. It is therefore on its own not more secure that "something you know", but should be combined with "something you know" to form a "two-factor" authentication system, in which a compromise of either one of the factors on its own would not be sufficient for an attacker to gain access.

Forms of token
There are a number of options on the market which could fulfil (or be seen to fulfil) "something you have" authentication. These forms of token can be broadly split into the following categories.

- Paper tokens: At the simplest level this could be a distributed list of "one time passwords", or could take the form of a "grid" of codes the user needs to enter in response to a form of challenge
- Soft tokens: These rely on a "software" component present on the client's computer, e.g. a cookie or a software token application
- Hardware tokens: These are physical devices the user needs to be in possession of. Typically hardware tokens will incorporate physical and logical mechanisms to protect their data and prevent copying.

One question to ask is, does the token actually implement the fundamental principles of "something you have" (and ONLY you have), i.e. Is the token unique?

Does the token have inherent protection against being copied, or if it was copied would this be apparent to the user?

If you cannot answer "Yes" to these questions, there can be no guarantee that ONLY you have that token. It would then have to be argued if the token could be considered as "something you have" for the purposes of authentication.

This effectively rules out any paper-based token, which can easily be copied. It may also eliminate any soft token unless it is securely linked to the hardware upon which it is installed (effectively making the computer hardware the token), which limits portability. Such token types may still have their merits in enhancing authentication, but are discounted for this discussion of "two-factor authentication" that requires you to physically have a token.

For choice of a secure two-factor (token-based) authentication mechanism it is therefore suggested that a hardware token is required.

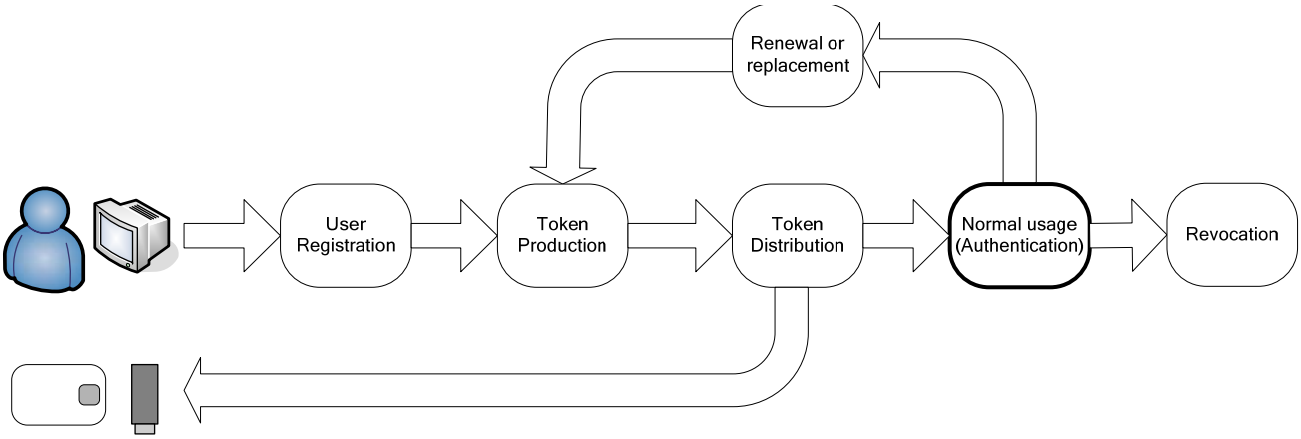

Diagram 1 - Processes in the lifecycle of a token

Hardware tokens
Hardware tokens can take many physical forms, e.g. a token that is (from the user's perspective) little more than a simple LCD display, a token that connects to a USB port, or a smart card. These tokens can operate in either a disconnected or connected manner. In general terms hardware tokens can be further sub-divided into the following categories:

- Disconnected tokens: These hardware tokens have no physical or logical connection to the client computer. Instead they generate authentication information which the user can manually enter as part of the authentication process
- Connected tokens: These are hardware tokens that need to be physically connected to the clients computer
- Contactless tokens: These are hardware tokens that logically connect to the client computer (like connected tokens), but do not require a physical connection.

Most disconnected tokens rely on a "one-time-password" (OTP) technique, i.e. on each use, they generate a new "one-time-password" password (PIN) that is valid only for that session and is derived cryptographically (i.e. cannot be easily predicted).

These OTP values may be derived based on time or sequence based information. More complex disconnected tokens may also use a "challenge-response" mechanism, if they have a keypad on which to enter a challenge presented from the web page before generating the response.

Connected tokens may make use of similar principles but with some added benefits:

- User interaction may be reduced, thus making the process simpler for users and reducing the likelihood of human error
- It is possible to use more cryptographically secure authentication of the token
- Enhanced functionality may be provided in the token, e.g. digital signature capability or additional functionality to combat phishing.

The issue with connected tokens is generally one of connectivity. Not all computers have smart card readers, and though most do have USB connectors these days, they cannot be guaranteed to be free to use or easily accessible. In a closed community, a connected hardware token, such as a smart card, is often an appropriate choice, but for the on-line community a disconnected token may be the best fit.

Contactless tokens have all the advantages of connected tokens, with the additional benefit that no physical connection is required. There is still the need to have the appropriate contactless card/token reader.

There is no single right answer to what is the best choice of token technology. The choice of token will vary according to application specific requirements, including usability, cost, and level of security. In some cases there may even be the need to support different token technologies for different users.

Supporting systems and processes
Traditionally a lot of the focus on "two-factor authentication" systems has been on the tokens themselves, however the implementation of supporting systems and processes can have as much of an impact on the user experience and the total cost of ownership of the system as the tokens themselves.

Any supporting systems and processes will need to securely manage a number of services which form part of the authentication system, throughout its lifecycle, which can include:

- User registration
- Token production and registration
- Token distribution
- User and token authentication
- Password changes and resets
- Token renewal
- Contingency for temporarily mislaid tokens
- Replacement of permanently lost or broken tokens
- User and token revocation.

The diagram at the top of this page summarises the processes in the lifecycle of the token.

Two-factor authentication

These processes have to be managed in a way that is scaleable for the target number of users (and beyond), meeting targets for performance and availability. For any large community it is likely that this will require a robust directory service to maintain the registration and authentication information. This may already be present for an existing user population, but may need some extension to support new authentication and token data. It should also be considered whether a new, dedicated, directory service could be required.

Interfacing into this directory service will be one or more systems for management of user and token life-cycle. These systems need to ensure the consistency of the data and as much as possible automate processes. If other systems or directories need to be linked into these processes, an identity management system may play an important role in streamlining the overall lifecycle management processes.

Finally, linking into the directory will be an authentication service to handle the authentication of the tokens. This will need to be integrated to the required access control systems or web servers (e.g. via the use of suitable plug-ins), and will also need to meet targets for performance and availability. The diagram on the right illustrates how these systems may link together.

Some important process decisions will need to be made including:

- What user registration processes are required, and how will these need to be secured?
- How are tokens to be issued (and re-issued) to end-users?
- What help-desk facilities will be required to deal with lost tokens and any authentication issues?

How will the above processes be secured to ensure tokens are only supplied to valid users?

In making these process decisions it should be considered whether these are aspects the organisation can take on-board themselves, or will parts of this need to be out-sourced? Does, for example, the token supplier have any facility for handling the issuance of tokens on the organisations behalf or can the system supplier provide any help-desk facilities?

Future proofing

To implement a two-factor authentication system, it can be a major investment. To gain a return on that investment it is important that the system will not become out-dated soon after it goes live. Any implementation should have one eye on future trends on how they may impact.

Questions you may want to ask include:

- Will the system scale if the number of users or transaction rate exceeds initial forecasts?
- How will the tokens or their lifecycle be affected as cryptographic attacks are enhanced?
- How much of the system implementation is standards-driven?
- Is there any potential for the system in the future to take advantage of any shared authentication tokens, which may help to amortise hardware token costs?
- Is there any possibility to extend the system to adopt external identity schemes (e.g. national schemes or EMV CAP)?
- Is there any capability to introduce new functionality to address new threats?

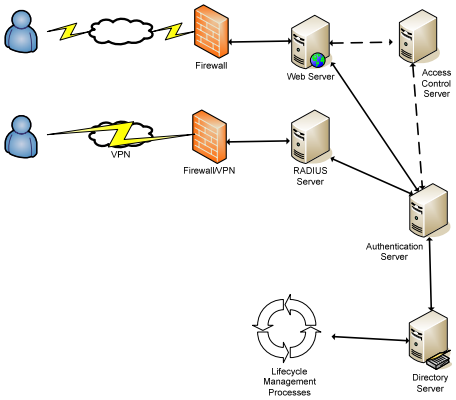

Diagram 2 - Systems linked together

Summary

A number of important decisions need to be made before embarking on a project to implement a two-factor authentication system. One of these is of course the choice of token, but this is not the only concern for the project. Of equal importance will be factors such as:

- What supporting systems will be put in place to manage the system?
- How will the various lifecycle processes work?
- Will any parts of the process need to be outsourced?
- Will any supplier be able to take ownership for the entire system, or will we need to deal with multiple point suppliers?
- What will the total cost of ownership of the system be, taking into account all the above factors as well as the token cost?
- How will the system cope with future trends?

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight