



Business case for Two-factor authentication (2FA)

Executive summary

Two factor authentication (meaning the use of security tokens in addition to usernames and passwords to authenticate computer users, principally customers accessing our Internet-facing systems) will reduce the possibility of identity theft and fraudulent abuse of customer accounts. The business case indicates a Net Present Value of \$??? over five years from an investment of \$???.

Introduction

Authenticating computer users, especially remote users accessing our networks and systems from the Internet or other third party networks, has traditionally been achieved by requesting usernames and passwords. However, passwords are only of value if they remain secrets, known only to the individual and our systems. If the user deliberately shares his password with someone else, our systems cannot differentiate them. If the user accidentally discloses his password, or if it is stolen by someone (e.g. using a "keylogger" on the user's PC), then the thief can also masquerade as the genuine user and we cannot tell them apart.

Deliberate theft of login details has become a serious problem. Identity theft is at an all time high and still climbing. Financial institutions are particularly vulnerable to frauds committed by identity thieves, or even by unethical customers who falsely deny their transactions and claim that 'someone else' must have withdrawn funds.

Background

Multifactor authentication offers a solution to the problems noted above by making it significantly more difficult to take over someone else's computer identity. 'Multifactor' refers to the use of additional methods of authentication besides usernames and passwords (which are 'something the user knows') – specifically 'something the user has' (meaning security tokens) and/or 'something the user is' (biometrics).

This paper makes a case for investing in two factor authentication (2FA) using security tokens to supplement usernames and passwords.

Business/Functional requirements

- Significantly reduce authentication failures, specifically false positives (*i.e.* someone falsely claiming to be another authorized user)
- Keep false negatives (*i.e.* failing to accept genuine authorized users) to an acceptable level
- Be manageable by employees
- Be usable by customers and other users
- Ability to manage tokens in issue e.g. disable lost/stolen tokens, replace broken tokens, report on tokens in use
- Ability to alter credit limits, transaction limits *etc.* according to whether a given customer uses a token or does not

- Ability to use the 2FA technology for other user authentication requirements such as privileged systems administrators, managers with purchasing and other authorities, *etc.*

Technical requirements

- Integrate readily with existing authentication and access control systems
- Comply with the organization's technical infrastructure architectural standards
- Comply with the organization's information security policies and standards
- Be scalable to suit differing levels of uptake
- Reflect current best practices and current/emerging technical standards

Costs

Implementation costs

- Specification and design
- Selection of technical solutions
- Development, customization, documentation *etc.* including adaptation of existing systems to suit 2FA
- Pre-production testing including pilot studies
- Rollout with enhanced implementation support

Operation costs

- Software license charges
- Hardware purchase charges (partially offset by customer charges)
- User provisioning including configuration and issue of new tokens, PIN codes *etc.*
- Procedures for configuring, issuing and managing tokens and PIN codes *etc.*
- Procedures to disable and re-issue lost/stolen/damaged tokens including replacement when the built-in batteries fail
- Reporting of tokens in use

Business benefits

Financial benefits

- Reduction in losses through frauds and thefts using compromised user details
- Competitive advantage over peer organizations that do not move to 2FA as quickly
- Greater sales through existing and new products and services due to security value

Intangible/nonfinancial benefits

- Greater confidence in the authenticity of users
- Greater ability to launch new remote access products and services
- Positioning as a security-conscious organization, with marketing advantages

Cost-benefit analysis

[Refer to spreadsheet analyzing the costs and benefits over 5 years, with a Net Present Value calculation using the organization's agreed Cost of Capital]

Recommendation

The Net Present Value of this proposal clearly supports the case for this investment purely on the financial analysis. The intangible/nonfinancial benefits noted above add more weight to the case.