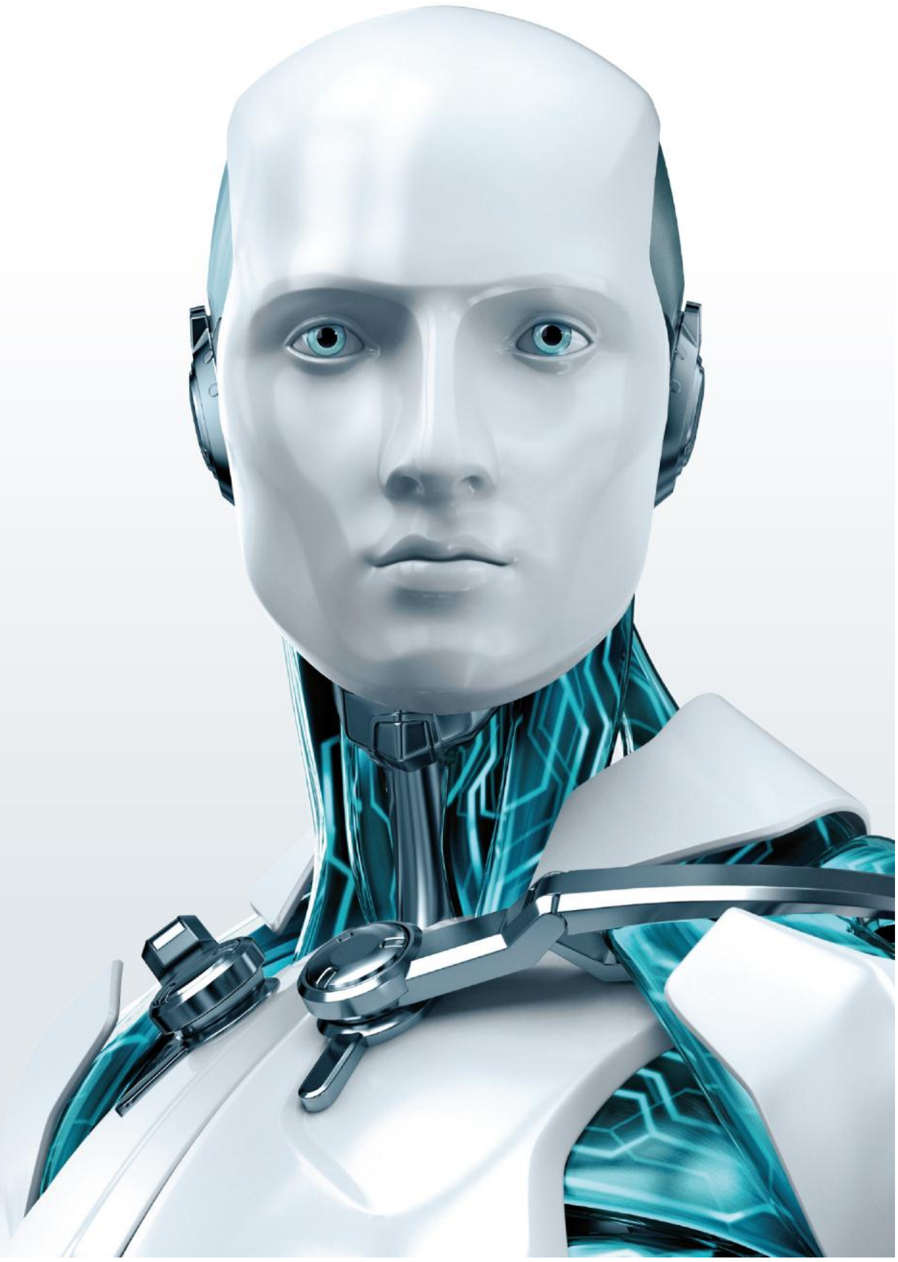
ESET Secure Authentication

Second factor authentication and compliance



Document Version 1.2

6 November, 2013

www.eset.com

Summary – second factor authentication and compliance

Region/Country	Legislation/ Guideline	ESET Secure Authentication meets explicit 2FA requirement	ESET Secure Authentication meets need for stronger authentication
International	ISO27001 Standard		✓
International	PCI/DSS - The Payment Card Industry Data Security Standard	✓	
International	ISAE 3402 – International Standards for Assurance Engagements no. 3402		✓
United States	HIPAA - Health Insurance Portability and Accountability Act		✓
United States	FFIEC - Federal Financial Institutions Examination Council compliances	✓	
United States	US Federal Government	✓	
United States	Sarbanes Oxley		✓
United Kingdom	"Code of Connection"		✓
South Africa	PPI - The Protection of Personal Information Act		✓

1. Introduction

The need to conform with regulatory, governance, compliance or audit standards has become a natural fact for most companies doing business in today’s dynamic corporate world. Increasingly many companies are equally obligated to comply with specific regulatory standards that govern their businesses.

This document attempts to assist these companies in this process by answering the following questions:

- What compliance requirements may your company be subject to?
- What do these requirements have to say about second factor authentication?

The intent is to map a path how you can easily leverage ESET Secure Authentication to conform to the various governing standards, thus raising their compliance footprint.

2. Compliance requirements

ISO27001 Standard (International)

The section on access control in the ISO 27002 code of practice for information security management describes access control requirements for external network connections. It is clear that this compliance standard regards external connections as a significant risk that requires deliberate controls to protect remote access. ESET Secure Authentication significantly enhances a customer's adherence to this requirement.

11 Access control
11.4 Network access control
b) appropriate authentication mechanisms are applied for users and equipment;
11.4.2 User authentication for external connections
Control: Appropriate authentication methods should be used to control access by remote users.
Implementation guidance: Authentication of remote users can be achieved using, for example,
a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions.

The section on physical entry access control is more explicit:

11.1.2 Physical entry controls
…access to areas where confidential information is processed or stored should be restricted to authorised individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism…

PCI/DSS - The Payment Card Industry Data Security Standard (International)

The payment card industry data security standard is the most explicit about 2FA:

Requirement 8: Assign a unique ID to each person with computer access

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial- in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication).

Note: Two-factor authentication requires that two of the three authentication methods be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.

When is Two-Factor Authentication Required?

All remote access to the PCI network must utilise two-factor authentication. In simple terms, remote access can be interpreted as any connection or access that crosses public networks. If any of the networks between the access source and Cardholder Data Environment (CDE) are considered to be public, or owned and operated by another entity, then the access should be considered remote. Virtual Private Networks (VPN) technologies create some interesting exceptions, as they effectively cause remote networks to behave like local networks.

For the purposes of requirement 8.3, point-to-point VPN technologies can be considered local network access, and Remote Access (RA) or client VPN technologies should be considered as remote. In both cases, you may need additional review to ensure that the controls adequately meet the intent of the requirement to utilize two-factor authentication for remote access to the CDE.

Common Misconceptions

One common misconception of Requirement 8.3 can be seen with the interpretation and definition of the term two-factor authentication. Some organizations interpret two-factor authentication to mean two authentication identifiers applied individually to two different authentication requests. In these cases, each authentication request only utilizes a single authentication identifier. Two single-factor authentication steps does not equal two-factor authentication.

Another common misconception is that Requirement 8.3 includes all access to the CDE, not just remote access. In these cases, organizations may deploy two-factor authentication mechanisms to authenticate access requests from all connected networks, including those that are locally connected. Although this is above and beyond the intent of requirement 8.3, this may improve and further secure access into the CDE.

Though adding additional authentication steps may improve the overall security of the remote access mechanisms, the improvement does not equal the improved security of a true two-factor authentication mechanism. The intent of requirement 8.3 is to ensure that two authentication identifiers are used within a single authentication request.

ISAE 3402 - International Standards for Assurance Engagements no. 3402 (International)

International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organisation, was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organisations and their auditors (user auditors) on the controls at a service organisation that are likely to impact or be a part of the user organisation's system of internal control over financial reporting.

Customers of ESET Secure Authentication that are "service organisations" that provide IT-related services to their customers may be required to implement controls to satisfy an ISAE 3402 audit. Access control is typically a key consideration of such an audit. 2FA on external access would enhance the ability of such a service organisation to obtain a favourable audit opinion.

HIPAA - Health Insurance Portability and Accountability Act (United States)

A US federal advisory group has endorsed requiring multi-factor authentication in certain cases for Stage 3 of the HITECH Act electronic health record incentive program that also governs IT services under HIPAA.

Stage 3 is slated to begin in 2015, and rules are in the early discussion stages at the Department of Health and Human Services.

FFIEC - Federal Financial Institutions Examination Council compliances (United States)

The U.S. Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.

Following the FFIEC publication advising the use of multi-factor authentication, numerous vendors began offering authentication solutions that are not compliant with the FFIEC's definition of "true multifactor authentication". Most notable of these approaches is the challenge/response approach, often coupled with a shared secret image. Soliciting personal information in response to challenge questions simply solicits more of "something the user knows", similar to a login, a password, or a PIN. All are multiple solutions from the same authentication category. Unless these are combined with one of the other two factors, i.e., "something the user has" or "something the user is," it does not constitute multi-factor authentication.

Regulators have repeatedly cautioned against the use of approaches that operate through the solicitation of personal information. On June 17, 2005, the U.S. Federal Deposit Insurance Corporation (FDIC) published supplement guidelines in which it strongly cautioned financial organisations against adopting authentication methods that use personal information for authentication purposes:

"Although consumers are worried about phishing and the trustworthiness of e-mail messages from their banks, they are also concerned about the security of their personal information more generally....When banks consider authentication methods for retail customers, they should be aware that these customers value security and the protection of confidential information... Consumers will require a clear explanation of any security mechanism and the use of any personal information required to implement that security mechanism....limitations on the use of personal information and the existence of privacy safeguards are important elements of consumer acceptance....Consumers are also concerned about the risk associated with large databases of personal information and the potential for the information that is used by authentication methods to be compromised, copied, or imitated. - FDIC"

The FFIEC clarified their position in their August 15, 2006 FAQ Supplement, rejecting such approaches outright:

"By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category ... would not constitute multifactor authentication. - FFIEC"

US Federal Government (United States)

IT regulatory standards for access to Federal Government systems require the use of two-factor authentication to access sensitive IT resources, for example when logging on to network devices to perform administrative tasks and when accessing any computer using a privileged login.

Sarbanes Oxley (United States)

Legislation from the Sarbanes-Oxley Act (SOX) requires that organisations use stronger forms of authentication to mitigate data theft, prevent fraud, and protect customer information and patient privacy.

“Code of Connection” (United Kingdom)

Second factor authentication helps organisations in the UK (e.g. councils) comply with the requirements of the “Code of Connection” which is mandated by online government services such as the UK Government Secure Extranet.

PPI - The Protection of Personal Information Act (South Africa)

The South African PPI legislation states that:

Principle 7 Security Safeguards
Security measures on integrity of personal information
18. (1) A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—
(b) establish and maintain appropriate safeguards against the risks identified;

It can be argued that given the weakness of password-only systems in today’s IT landscape (particularly related to password reuse) a responsible organisation should implement 2FA (among other things) to reduce the risks against personal information under their control.