



MODULE	OM: Operational Risk Management
CHAPTER	OM-3: Electronic Financing Activities

## OM-3.2 Secure Authentication

### OM-3.2.1

Licensees must take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business. Licensees must, at a minimum, establish adequate security features for customer authentication including the use of at least two of the following three elements:

- (a) knowledge (something only the user knows), such as pin or password;
- (b) possession (something only the user possesses) such as mobile phone, smart watch, smart card or a token; and
- (c) inherence (something the user is), such as fingerprint, facial recognition, voice patterns, DNA signature and iris format.

### OM-3.2.2

For the purpose of Paragraph OM-3.2.1, licensees must ensure that the authentication elements are independent from each other, in that the breach of one does not compromise the reliability of the others and are sufficiently complex to prevent forgery.



MODULE	RM:	Risk Management
CHAPTER	RM-1:	General Requirements

## RM-1.5 Operational Risk

### *Secure Authentication*

#### RM-1.5.7

Licensees must take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business. Licensees must, at a minimum, establish adequate security features for customer authentication including the use of at least two of the following three elements:

- (a) knowledge (something only the user knows), such as pin or password;
- (b) possession (something only the user possesses) such as mobile phone, smart watch, smart card or a token; and
- (c) inherence (something the user is), such as fingerprint, facial recognition, voice patterns, DNA signature and iris format.

#### RM-1.5.8

For the purpose of Paragraph RM-1.5.7, licensees must ensure that the authentication elements are independent from each other, in that the breach of one does not compromise the reliability of the others and are sufficiently complex to prevent forgery.



MODULE	GR:	General Requirements
CHAPTER	GR-12:	Information Security

## GR-12.1 Electronic Frauds

### *Secure Authentication*

#### GR-12.1.3

PSPs and crowdfunding platform operators must take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business. Licensees must, at a minimum, establish adequate security features for customer authentication including the use of at least two of the following three elements:

- (a) knowledge (something only the user knows), such as pin or password;
- (b) possession (something only the user possesses) such as mobile phone, smart watch, smart card or a token; and
- (c) inherence (something the user is), such as fingerprint, facial recognition, voice patterns, DNA signature and iris format.

#### GR-12.1.4

For the purpose of Paragraph GR-12.1.3, PSPs and crowdfunding platform operators must ensure that the authentication elements are independent from each other, in that the breach of one does not compromise the reliability of the others and are sufficiently complex to prevent forgery.