

VETT
Much more than 2 factor authentication

Wikipedia offers a definition for two factor authentication as follows:

There are three universally recognized factors for authenticating individuals:

- 'Something you know', such as a password, PIN or an out of wallet response.
- 'Something you have', such as a mobile phone, credit card or hardware security token.
- 'Something you are', such as a fingerprint, a retinal scan, or other biometric.

New category

VETT enables a new category termed 'Something you control' such as the communication address for a device or drop box.

Account set up

VETT draws on the User's relationship with a financial institution (Bank) to authenticate and to connect the User, and then provide access to the data server. (The VETT server receives transaction data from Service Providers this transaction data is stored pending authorisation). When a User sets up their account the financial institution will ask the User to specify an email address and a mobile number (communication addresses) this data forms part of the security net for the User's protection. The same or a different number/email will be registered as notification address.

Communication and notification

User may change a communications address with VETT (place an instruction, receive and review, then connect authenticate and authorise) to maintain security and control. A copy instruction which requires the User's authorisation can only be delivered to the current registered communications address. All instructions authenticated and/or authorised via the financial institution generate a notification message.

Why notification

If your wallet is lost or stolen you will be aware of the loss within a short space of time. The loss is obvious. However, if someone uses your credit card account number the chances are that you will not be aware of any fraudulent activity until sometime later, much later. Such a theft will only become apparent when and if you review and verify all entries on your monthly credit card statement.

Something you control

VETT can incorporate the three factors as noted above and further include this new factor of 'Something you control' which could be a secure email address and/or mobile phone number. Control is assured, first a User must have access to use a VETT enabled account, secondly they must have access to the communications address and then there is the notification message.

VETT is designed to protect a User when they engage in remote commerce, and to thwart cyber and other such attacks.

Controversial

VETT can therefore demonstrate three factor protection for a transaction but the "experts" have still to agree amongst themselves and accept the concept of 'three factor authentication'

Research notes

Two-factor authentication (T-FA)

In order to understand Two-factor authentication, it's important to understand the three methods by which people authenticate themselves to digital systems:

There are three universally recognized factors for authenticating individuals:

- 'Something you know', such as a [password](#), [PIN](#) or an [out of wallet](#) response.
- 'Something you have', such as a [mobile phone](#), [credit card](#) or hardware [security token](#).
- 'Something you are', such as a fingerprint, a [retinal scan](#), or other [biometric](#).

A system is said to leverage Two-factor authentication (T-FA) (or dual factor authentication) when it requires at least two of the authentication form factors mentioned above. This contrasts with traditional [password](#) authentication, which requires only one [authentication factor](#) (such as knowledge of a [password](#)) in order to gain access to a system.

Common implementations of two-factor authentication use 'something you know' (a [password](#)) as one of the two factors, and use either 'something you have' (a physical device) or 'something you are' (a [biometric](#) such as a fingerprint) as the other factor. A common example of T-FA is a bank card ([credit card](#), [debit card](#)); the card itself is the physical "something you have" item, and the [personal identification number](#) (PIN) is the "something you know" password that goes with it. See [Chip and PIN](#) for more information on this.

Using more than one factor is also called strong authentication; using just one factor, for example just a [static password](#), is considered by some to be [weak authentication](#). (Strong authentication also includes multi-factor that do not include a physical factor, such as a card or [dongle](#). The multiple factors can both be online for strong authentication.)

According to proponents, T-FA could drastically reduce the incidence of online [identity theft](#), and other online [fraud](#), because the victim's password would no longer be enough to give a thief access to their information. However, T-FA is still vulnerable to [trojan](#) and [man-in-the-middle attacks](#).

(In [cryptography](#), a [man-in-the-middle attack \(MITM\)](#) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against [public-key cryptography](#) and is also particularly applicable to the original [Diffie-Hellman key exchange](#) protocol, when used without authentication.

Deployment of T-FA tools such as [smart cards](#) and [USB tokens](#) appears to be increasing. More organizations are adding a layer of security to the [desktop](#) that requires users to physically possess a token, and have knowledge of a PIN or password in order to access company data. However, there are still some drawbacks to two-factor authentication that are keeping the technology from widespread deployment. Some consumers have difficulty keeping track of one more object in their life. Also, many two-factor authentication solutions are proprietary and protected by [patents](#). The result is a substantial annual fee per person protected and a lack of [interoperability](#).

Authentication factor - From Wikipedia, the free encyclopedia

In [authentication](#), a factor is a piece of information used to verify a person's identity for security purposes.

The three most commonly recognized factors are:

- 'Something you know', such as a [password](#) or [PIN](#)
- 'Something you have', such as a [credit card](#) or [hardware token](#)
- 'Something you are', such as a fingerprint, a [retinal](#) pattern, or other [biometric](#).

Other, less common factors may include:

- Recognition-based or *cognometric* authentication, such as Passfaces™, where the user has to recognize pre-assigned secret faces
- [Cybermetric authentication](#), such as only allowing access from the certain computer, which is the combination of unique hardware and (or) software installed
- [Location-based authentication](#), such as only allowing a particular atm, charge, or credit card to be used at a specific merchant or at a specific bank branch, or only allowing root access from specific terminals
- [Time-based authentication](#), such as only allowing access from certain accounts during normal working hours
- [Size-based authorization](#), such as only allowing a specific transaction to be for a specific exact amount
- [Pre-authorized transactions](#), such as where a company uploads all of the check numbers and amounts written for each check to their bank, and the bank would then reject any check not of those numbers and amounts as fraudulent

Types of authentication

Biometrics

E-mail authentication

Identity management

Identity management systems

License plates

Message authentication codes

Personal identification

Seals

Smart card

Watermarking