

# Two-Factor Authentication

*Last reviewed: July 2015*

## What Is Two-Factor Authentication?

It is the use of two independent means of evidence (factors) to assert the identity of a user requesting access to some application or service to the organization that provides the application or service. The objective of two-factor authentication, as a method of electronic computer authentication, is to decrease the probability that the requestor is not who he/she claims to be (i.e., providing false evidence of his/her identity.) Two-factor authentication is achieved by a combination of any two of the three "Somethings" below:

### Something you know

- Personal Identification Number (PIN)
- Password

### Something you have

- Smartphone
- Token
- ID Badge / Smart card

### Something you are

- Fingerprint
- Retinal Scan
- Voice Pattern
- Typing Cadence

Note that the use of a password in combination with a PIN, for example, is NOT considered two-factor authentication because both pieces of information involve a single factor - something you know.

The use of two-factor authentication has been pervasive and ubiquitous for quite a long time already. Any person who has used an ATM machine to withdraw cash for a bank account has used two factor authentication – you had to provide something you had (a card) and had to provide something you know (a PIN) in order to complete the transaction.

## What Is The Difference Between Two-Factor and Multi-Factor Authentication?

The subtle difference is that, while two-factor authentication uses exactly two factors to assert the identity of a user, multi-factor authentication uses two or more factors to assert identity. In essence, two-factor authentication is a subset of multi-factor authentication. An example of multi-factor authentication would be the requirement to insert a smart-card (something you have) into a smart-card reader, enter a PIN (something you know), and provide a valid fingerprint (something you are) provided via a biometric fingerprint reader. This example uses three factors to assert the identity of a user.

## What are the Business Reasons to Consider Two-Factor Authentication?

Privacy, and the threat of identity theft, is increasingly a concern as more of personal information finds its way to online applications. In addition, passwords alone can frequently be easily guessed or compromised through phishing or hacking, consequently, no longer providing adequate protection for mission-critical information system and applications containing Personally Identifiable Information (PII), Personal Health Information (PHI), and other confidential information. Some specific concerns:

- As passwords become easier to guess or compromise, password complexity requirements are quickly coming to exceed what users can reasonably remember.
- Password proliferation has increased the time and effort spent on user support because of forgotten passwords and the need to reset them.
- Many password reset mechanisms are insecure, even if the passwords themselves are not.
- The increased use of single sign on increases the value of passwords and the number of ways by which those passwords can be potentially attacked.
- Passwords are all-too-often cached in applications (e.g., email clients or web browsers), stored off site (e.g., POP/IMAP consolidation of email from multiple accounts), and reused for multiple services, some highly sensitive.

See [Passwords](#), a presentation at the NWACC Security Conference 2009, for a in-depth review of all the reasons why it makes good business sense to consider two-factor authentication as alternative to traditional passwords.

Compliance is also driving adoption of two-factor authentication in other areas – three examples:

- The Federal Information Security Management Act (FISMA) applies to grantees (e.g., institutions of higher education) when they collect, store, process, transmit or use information on behalf of the United States Department of Health and Human Services (HHS) or any of its component organizations. In other words, Federal security requirements apply and the institution of higher education is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III and [NIST SP 800-63 Electronic Authentication Guideline](#)).
- The Health Insurance Portability and Accountability Act (HIPAA), where the most important concern is the confidentiality of patient records and protected health information, does not explicitly require two-factor authentication but clearly makes an appeal to the use of industry best standards.
- The Payment Card Industry Data Security Standard (PCI DSS), where the most important concern is the confidentiality of cardholder information, hints at the desirability of using multiple factors in its requirement 8.2 "In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric." It is more specific in its requirement 8.3 regarding remote access to the local network

"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 dialin service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)"

Other requirements for two-factor authentication include Internet banking. For that reason, the Federal Financial Institutions Examination Council (FFIEC) strongly recommends two-factor authentication for consumer online banking services. Specifically, in its [Supplement to Authentication in an Internet Banking Environment](#), under Customer Authentication for High Risk Transactions, it states "Financial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered business transactions. Additionally, the Agencies recommend that institutions offer multi-factor authentication to their business customers."



#### Additional Resources

Check out [Breaking the Ubiquitous Two-Factor Barrier](#), presented by Jane Drews (University of Iowa and Quinn Shamblyn (Boston University) at the 2015 Security Professionals Conference. For other recent presentations visit [access control](#) and [identity and access management](#) in the EDUCAUSE library.

Learn more about [Two-Factor Authentication with Duo Push](#) by visiting the [Internet2 NET+ website](#).

Also see [Client \(Personal\) Certificates: Should We Be Thinking About Certificate Use Cases or Should We Be Thinking About The Sort of Credential Deployment Model We Need?](#) (a presentation at the 2011 Internet2 Member Meeting) for questions to ponder when considering deployment of two-factor authentication.

## What Technology Is Available?

### 1. Second Channel Authentication - Mobile Phone-based

Though similar to two-factor authentication but different, second channel authentication allows individuals to use their mobile phone as a security token (i.e., what you have.) A Java application installed on the mobile phone performs the functions normally provided by a security token. Other methods of using the cell phone include using Short Message Service (SMS) messaging, prompting an interactive telephone call, or using standard Internet protocols such as HTTP or HTTPS. Second channel authentication uses a mobile phone via a cellular network in addition to the computing device connected via an IP connection. This authentication method is already in use in online shopping, with Google's version of two-factor authentication built within the Google shopping cart.

See [Mobile One-Time-Passwords \(OTP\)](#), [Google Authenticator](#), and [DuoSecurity](#) for information on implementation of OTP via mobile phones. Additional implementation options include:

- SMS push to a preregistered device
- Photograph-the-barcode-on-your-device's screen
- Answer a call made to the individual's mobile phone and hit a specified key
- Biometric voice verification

#### *Advantages:*

- Since most users are already carrying smartphones, it may be perceived as an easier or more convenient way to authenticate than using tokens or smart cards
- Compatible with a large number of applications
- Easy to use

#### *Disadvantages:*

- Relatively new technology, not as mature but gaining acceptance
- Some confusion exists regarding the levels of two-factor strength of DTMF tones (out of band) vs one-time-passwords (in band) vs SMS (either or) and vendor available options
- The possibility of cell phone cloning or interception
- There may be locations/situations in which the use of smartphones may not be viable or functional (airplanes? basements?) or may be too expensive (e.g., when travelling overseas and paying international rates/roaming rates)

#### *Who Is Using It (this is just a sample list):*

- [Boston University](#)
- [University of Colorado](#)
- [University of Iowa](#)

### 2. Security Tokens

A small device that an individual possesses and controls used to authenticate the individual's identity. It provides the "what you have" component of two-factor authentication since it is used in addition to another piece of evidence (e.g., a password) to prove that individuals are who they claim to be. A token generates a unique code that is combined with an individual's password to create an electronic "ticket" that authenticates the individual and encrypts the transmission to ensure data integrity. Security tokens come in different types. The most common are:

**Hardware Tokens:** Physical devices small enough to be carried in a pocket or attached to a keychain. They may store digital credentials, a digital certificate, or digitized biometric data (e.g., a fingerprint). Some hardware tokens include input and output interfaces like a small keypad to enter a PIN or a button to generate a key number and a display window to show it. They can also include a Bluetooth wireless interface to enable transfer of the generated key number to a client system.

Hardware tokens also come in different types. Some of the most common are:

- One Time Password (OTP) tokens which generate a new password every so many seconds.
- Challenge-Response tokens, which, given an input (such as a random string of numbers) provide a unique response, which can then be validated by the authenticating server
- USB hard tokens. See description below.
- Other technology solutions such as grid cards or Personal Identification Number (PIN) / Transaction Authentication Number (TAN) systems

*Advantages:*

- Mature technology
- Compatible with a large number of applications
- Easy to carry
- Strong second factor

*Disadvantages:*

- Easily lost and/or forgotten
- Medium/high time and effort to deploy and maintain
- Comparatively medium/high cost of ownership / deployment though purchase costs are declining.

*Who Is Using It (this is just a sample list):*

- [University of Michigan MToken](#)
- [University of Michigan MToken \(article\)](#)

**USB Token:** A specific type of hardware token designed to include a Universal Serial Bus (USB) connector. A USB port is standard equipment on today's computers. USB tokens are normally used to store digital certificates. They plug into a computer's USB port and, in some cases, individuals are prompted to enter their PIN to unlock/pass the digital certificate.

Some USB tokens may need drivers to be installed while others may come with self-installing drivers but that only work with certain versions of Windows.

*Advantages:*

- Mature technology
- Easy to Carry
- Strong second factor

*Disadvantages:*

- Easily lost and/or forgotten
- Comparatively medium / high cost of ownership / deployment
- Can be time consuming to maintain
- Requires USB port (or adapter) on the user device

*Who Is Using It (this is just a sample list):*

- [Dartmouth and UT System](#)
- [Virginia Tech](#)

**Software Tokens:** Non-physical device that is stored on a desktop computer, laptop, Personal Digital Assistant (PDA), or mobile phone. As in the case of hardware tokens, they may store digital credentials or a digital certificate.

*Advantages:*

- Comparatively lower cost of ownership / deployment
- Compatible with a large number of applications
- Easier to deploy than a hardware token

- Strong second factor but not as strong as hardware token

*Disadvantages:*

- Some argue that a software token can be copied so they're not a true version of "something you have"
- Can be time consuming to maintain
- Software tokens stored on-devices are less secure than software tokens stored off-devices (e.g., hard tokens)

*Who Is Using It (this is just a sample list):*

- [University at Buffalo](#)

### 3. Smart Cards

A pocket-sized card, similar to credit card, with embedded integrated circuits that communicate with external devices via a card reader.

Smart cards can be programmed to provide identification and authentication services. The most advanced cards include encryption hardware that uses algorithms that support the NIST standard for Personal Identity Verification (FIPS 201) and/or secure Bluetooth-enabled card readers to link smart cards to users' smart phones but the readers can be expensive.

Similar to USB tokens, they also provide the "what you have" component of two-factor authentication since with a smart card an individual authenticates by using a PIN in combination with a smart card that contains the individual-specific information.

*Advantages:*

- Easy to carry
- Can be tied to physical security strategy (ID Badge)
- Strong second factor with use of PIN
- Use of encryption, therefore the information is more secure.

*Disadvantages:*

- Cards can be lost or stolen
- Comparatively medium / high cost of ownership / deployment
- Smartcards need card readers

*Who Is Using It (this is just a sample list):*

- [University of Central Florida](#)

### 4. Biometrics

The use of intrinsic physiological and behavioral characteristics to authenticate a particular individual. Most biometric-based authentication follows a four-step process:

1. Create a sample of individuals' biometric characteristics during an enrollment process. A profile of an individual's characteristics can be built based on a specific number of samples given.
2. Unique data are extracted from the sample and a template is created.
3. The template is compared with a new sample provided during authentication.
4. Access is determined by matching the features extracted from the new sample with those of the template.

*Advantages:*

- Strong second factor
- Meet security requirements of integrity and nonrepudiation when combined with digital signatures

*Disadvantages:*

- Requires relatively more complex and expensive technology
- Requires calibration through multiple image captures to minimize the probability of erroneous rejection of authorized individuals or erroneous acceptance of unauthorized individuals
- Concerns about accuracy, privacy and security of biometric indicators, and potential inconvenience make user acceptance difficult
- Adds complexity to replacement of compromised credentials (e. g., how do you revise the template created from an individual's iris scan or thumbprint)
- Illness or injury might make it difficult or impossible for individuals to authenticate
- Potential accessibility barriers for disabled individuals

## Questions to Ask IF Selecting Biometrics



- Would my institution provide effective notice and an opportunity for meaningful consent prior to collecting a biometric sample?
- Is my institution selecting the most appropriate **and** least intrusive biometric to address the business need?
- What alternative(s) are acceptable/provided for those who may refuse or are unable to provide the selected biometric image?
- Would my institution be generating and encrypting an alphanumeric identifier from the raw/scanned image and would it be using a unique algorithm to limit the identifier's utility outside of the intended domain?
- Would my institution be retaining only the encrypted, alphanumeric identifier and not the raw/scanned image?
- Would the selected identifier-creation algorithm ensure an adequate level of uniqueness, i.e., can different images produce the same identifier?  
Corollary: Is absolute uniqueness really critical, especially in situations where the identifier is used in conjunction with a second credential, such as a PIN or password?
- Would my institution be considering or using "no trace" technology rather than embedding the digitized identifier into a microchip or smart card?
- Would institutional staff responsible for capturing and manipulating the raw images and identifiers be appropriately trained on the confidentiality and appropriate use of these data?
- How would my institution appropriately destroy the raw images and/or the identifier once their purpose has been served?
- Would my institution create, implement, and maintain policies and procedures for the collection and management of biometric data? How often would these policies and procedures be audited or assessed regarding changes in technology, best practices, and the legal/regulatory environment?


## A number of biometric technologies measure different physiological and behavioral aspects of an individual

	Fingerprint Recognition	Signature Characteristics	Palm Scan	Hand Geometry	Retina Scan	Iris Scan	Keyboard Dynamics	Voice Print	Facial Scan
<b>Descripti on</b>	Examines the unique ridge endings and bifurcations displayed by friction ridges of an individual's fingerprint	Often referred to as dynamic signature verification (DSV), examines how individuals sign their names	Examines the unique creases, ridges, grooves in an individual's hand. Also scans the fingerprints of each finger.	Examines the length and width of an individual's hand. The system compares the geometry of each finger and the hand as a whole	Examines the blood vessel patterns of the retina on the backside of the eyeball	Examines the colored portion of the eye that surrounds the pupil. The iris has unique characteristics (e.g., colors, rings, etc).	Examines the speed and motion used by an individual when typing a specific phrase	Examines an individual's speech sounds and patterns when saying a sequence of words	Examines facial characteristics of an individual - bone structure, nose ridge, eyes width, forehead size, etc.
<b>Accuracy</b>	High accuracy level. Standards based on the FBI Automated Fingerprint Identification System (AFIS).  Important to note that not all fingerprint recognition technology is the same and is equally accurate.	Low accuracy level		Medium/ Low accuracy level despite highly stable pattern over individual life	The most accurate biometric authentication	The second most accurate biometric authentication. Iris remains unchanged throughout life so iris scan has longer useful life.	Low level of accuracy. Subject to significant variances due to changes of behavior and posture	Medium accuracy level. Can be impacted by circumstances like a cold	Medium / low accuracy level. Pretty good at full frontal views but has problems with angle views, profiles, and varying facial expressions
<b>User acceptance</b>	Average acceptance though it is the most used and most practical biometric	Very high acceptance level. The signature is the most common form of authentication in the paper world	Average acceptance	High acceptance	Least level of user acceptance	Average acceptance	High acceptance	High acceptance	Average acceptance
<b>Relative Cost</b>	Medium / Low	Medium		Medium	High	High	Low	Medium	Medium
<b>Application in interface</b>	Scanner. Easy to use and require little space	Optic pen and touch panel. More sophisticated devices can measure: the angle of the pen, the pressure applied, the time taken to sign, and the velocity and acceleration of the signature	Scanner	Scanner. Easy to capture but system requires large physical space	Reader. Requires direct contact with a cup reader	Reader. Does not require direct contact with the reader	Keyboard	Microphone or telephone. Commonly available sensors Hands-free and eyes-free operation	Camera
<b>Special Requirements</b>		Requires individuals to sign their name with a special pen on a sensitized reader or pad				Acquisition of iris image requires more training than most biometrics			
<b>Privacy</b>	Privacy concerns of criminal implications		Same as fingerprint		Can reveal personal medical	None. Does not reveal personal medical conditions			

y C o n c e r n s					conditions like high blood pressure and pregnancy				
---	--	--	--	--	--	--	--	--	--

Sources: [The Biometrics Consortium](#); [The Biometrics Research Group](#); [Biometrics.gov](#) [Biometrics Overview](#); and James Michael Stewart, Ed Tittle, Mike Chapple "CISSP Study Guide", Third Edition

 Questions or comments?  [Contact us](#).

 Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License ([CC BY-NC-SA 4.0](#)).