Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update

FOUNDATIONAL **Refreshed:** 4 December 2020 | **Published:** 19 September 2011 **ID:** G00219391

Analyst(s): Ant Allan

This research identifies the limitations of counting authentication factors as an indicator of authentication strength, describes what contributes to authentication strength and outlines how the strength of a particular authentication method can be evaluated. Enterprises must make properly informed decisions when selecting new authentication methods, and not assume that a "two factor" authentication (2fa) method is necessary or sufficient in any particular use case.

FOUNDATIONAL DOCUMENT

This research is reviewed periodically for accuracy. Last reviewed on **4 December 2020**.

Key Findings

- There is no transparent, formal methodology for evaluating authentication strength. Standards and guidelines that classify authentication methods generally lack a clear basis.
- The familiar triplet of authentication factors (that is, distinct kinds of authentication attributes: something known, something held or something inherent) is part of the canon of information security. However, simply counting authentication factors doesn't tell us much about the strength of any authentication method.
- Many end users, vendors and regulators use "two-factor authentication" without a clear understanding or definition of the term.
- Additional information related to users and the context of their access can provide additional corroboration of users' claimed identities and, thus, can be regarded as a different grade of authentication attributes.

Recommendations

- When matching authentication methods to your needs for assurance and accountability, don't assume that any "two factor" method is automatically good enough, or that any "single factor" method isn't. Nevertheless, you may be obliged to select a "two factor" method by regulatory compliance requirements.
- Consider how other user attributes or contextual information can be folded into an authentication decision to improve the level of confidence in users' claimed identities.
- Carefully evaluate the strength of any candidate authentication method as it will be implemented in any given use case to confirm that it meets your needs for assurance or accountability.

Analysis

Authentication is the real-time process of corroborating a claimed digital identity with a specified or understood level of confidence (see Note 1), which enables activity to be (equally confidently) attributed to a specific individual and militates against illicit access. It is widely accepted that the strength of an authentication method — a measure of the level of confidence in a claimed identity that the method provides — is directly related to the number of authentication factors used, a notion that is entrenched in many regulations. However, the number of factors is neither the sole basis nor a direct indicator of authentication strength, and finding an authentication method that provides the right strength (that is, what's appropriate to the level of risk in a particular use case) is ultimately more important to an enterprise than the number of factors a method has. What, then, is the significance of authentication factors?

The sad truth is that counting authentication factors is important only to meeting the letter of some regulatory compliance requirements.

Authentication Strength

Authentication may be undermined by two kinds of attacks:

- *Masquerade attacks,* in which an attacker is (by some means) able to corroborate a falsely claimed digital identity and, thus, log in as a legitimate user.
- *Session hijacking attacks,* such as a man-in-the browser attack, which take control of or parasitize an already-authenticated session after a legitimate user's claimed digital identity has been corroborated.

Note that session hijacking attacks bypass authentication and, thus, can succeed no matter how strong the authentication method is. (Thus, there is always a need for fraud detection, misuse monitoring and other compensating controls, as discussed in other Gartner research, such as "Where Strong Authentication Fails and What You Can Do About It." [Note: This document has been archived; some of its content may not reflect current conditions.])

Authentication strength, therefore, measures only how hard it is for another person to masquerade as the legitimate user.

This has two aspects:

1. *The method's resistance to attack* — that is, how hard is it for an attacker to directly compromise or undermine the authentication method (without the user's knowing collusion)?
2. *The method's resistance to willful misuse* — that is, how hard is it for a user to deliberately allow colleagues and others to share his or her account?

Authentication strength is often more formally expressed as a *level of assurance* (see, for example, NIST SP 800-63-1, "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, Draft 3"). Gartner research also considers *level of accountability* as a distinct (but not wholly orthogonal) expression of resistance to willful misuse.

Authentication Factors

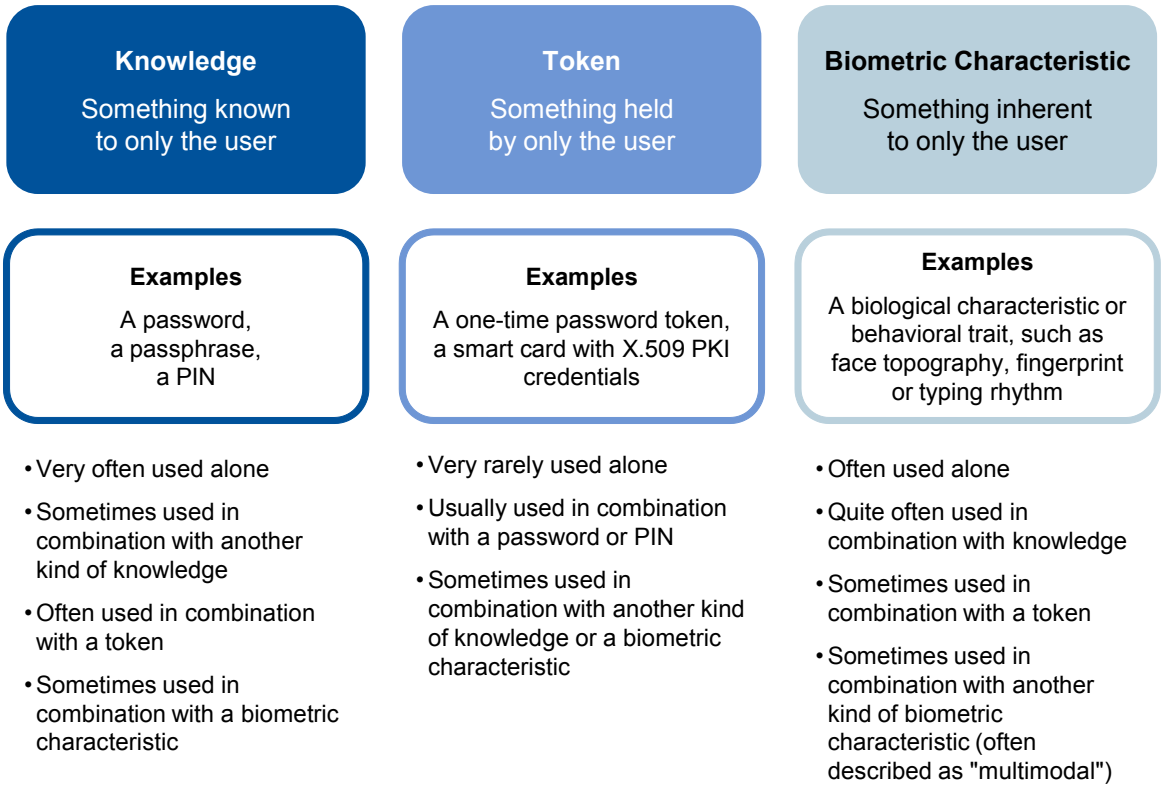
Traditional authentication methods are based on something uniquely possessed by the user — one or more *authentication attributes,* often called *credentials* or *tokens* (in this context, "token" doesn't imply a physical device) — which map to some information associated with and bound to a corresponding digital identity. When the user authenticates, he or she provides some evidence to prove possession (*authentication information,* typically derived from the authentication attributes), and the authentication service verifies that evidence based on the corresponding information bound to the user's digital identity.

It is widely accepted that authentication methods can be characterized by three kinds of authentication attributes, or three authentication factors — a description that goes back at least as far as the Federal Information Processing Standards (FIPS) Publication (Pub) 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," 30 May 1975 (see Note 2):

1. *Something known* to only the user — for example, a password, a passphrase, a personal identification number (PIN), a pattern or a picture.
2. *Something held* by only the user — for example, a token, such as a one-time password (OTP) token or a smart card with X.509 public-key infrastructure (PKI) credentials. More precisely, the authentication attribute is the cryptographic key (or similar) stored in the token, rather than the token itself.
3. *Something inherent* to only the user — that is, a biometric characteristic, such as face topography, fingerprint or typing rhythm.

An authentication method may be based on a single authentication attribute of any kind (although authentication based on a token alone is rare), or on two or more attributes of the same kind or different kinds (see Figure 1).

Figure 1. The Canonical Three Authentication Factors



Source: Gartner (September 2011)

Combining Authentication Attributes

Combining two or more attributes of the same kind potentially increases authentication strength, compared with using either one alone (although Prof. John Daugman of the University of Cambridge has shown that combining two different biometric characteristics can, in some instances, yield a method that's weaker than the stronger single-characteristic method). For example, simple passwords are vulnerable to keyboard-logging software; however, adding a second, partial password entered via drop-down menus thwarts this particular attack. This approach has been successfully used by some retail banks to reduce online banking fraud. However, because each kind of authentication attribute has a set of common, intrinsic vulnerabilities, a combination of two attributes of the same kind (that is, two instances of the same factor) will share many of the same vulnerabilities (for example, an attacker may discover multiple knowledge attributes by social engineering).

Only by combining attributes of different kinds (that is, different factors) with different (nonoverlapping) sets of vulnerabilities is there a *significant* increase in resistance to attack and, thus, in authentication strength. Hence, the resulting 2fa and *three-factor authentication* (3fa) methods are widely regarded as "strong," and the terms are taken as equivalent to the term "*strong authentication*." The notion that 2fa is strong is reflected in the many regulations that mandate the

use of 2fa, although this term isn't always well-defined in the regulations (the first version of PCI Data Security Standard was notoriously bad in this respect).

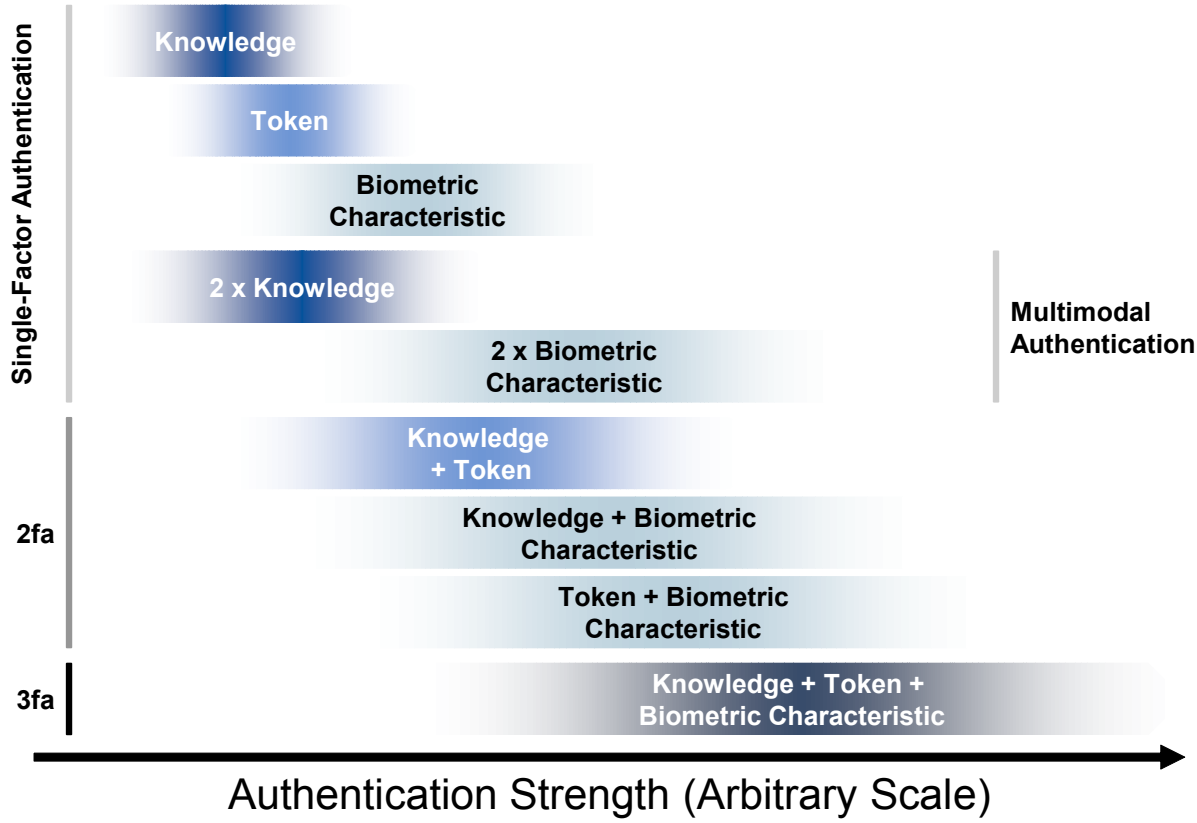
However, any 2fa (or even 3fa) method isn't *necessarily* stronger than an authentication method based on a single-authentication attribute:

- While 2fa is potentially stronger than authentication based on either of the two factors alone, authentication based on another independent factor might be stronger. For example, a robust biometric authentication method using vein structure is likely stronger than a "legacy password plus OTP grid card" method.
- A 2fa method may be no stronger than one of its components used alone, at least with regard to some kinds of attacks. For example, a "fly-phishing" attack that captures and immediately (mis)uses an OTP will be equally successful whether the OTP token was PIN-protected or not.

Furthermore, authentication methods that combine two attributes of the *same* kind are often erroneously presented by vendors, or accepted by enterprises, as 2fa methods. Thus, an enterprise may be duped into implementing an authentication method that doesn't comply with the regulation (but that may or may not meet its own authentication needs).

In summary, the number of factors (that is, distinct kinds of authentication attributes) is neither the sole basis nor a direct indicator of authentication strength. 2fa and 3fa do not indicate discrete, stepwise improvements in authentication strength, but yield overlapping continua (see Figure 2).

Figure 2. Notional Authentication Strength of Different Combinations of Authentication Attributes



Source: Gartner (September 2011)

Are There More Than Three Authentication Factors?

Vendors and others sometimes assert the existence of other kinds of authentication factors, such as:

- *Endpoint identity (EPI)* via X.509 credentials, a cookie or other software "blob," or a signature generated from unique hardware and software characteristics
- Geolocation, derived from an IP address
- Behavior (distinct from a behavioral biometric characteristic), such as transaction patterns.

However, these "factors" are unlike the canonical factors because there is no authentication attribute (such as a password, a cryptographic key or a biological characteristic) bound to and uniquely associated with the user. Nevertheless, they provide contextual information that can be folded into an initial authentication decision (based on canonical factors) or a subsequent access control decision. This approach is embraced in Web fraud detection (WFD) and other adaptive access control tools (see "Magic Quadrant for Web Fraud Detection," "The Future of Information Security Is Context Aware and Adaptive" and "Adaptive Access Control Emerges" [Note: This document has been archived; some of its content may not reflect current conditions]).

Such contextual information can be interpreted in two ways that are conversely related to each other. First, some kinds of contextual information can indicate increased risk associated with the user's access — for example, transaction anomalies. If the risk crosses a specified threshold, then the user might be prompted to reauthenticate with a higher assurance method or verify transaction details, or their access may be more rigorously audited or blocked altogether.

Second, while a WFD tool may normally be configured to interpret an *unknown* endpoint as indicating increased risk, a *known* endpoint can indicate increased confidence in a claimed identity. As with canonical authentication attributes, different instances of EPI provide different degrees of corroboration: A PC within the enterprise's office that is accessible to all employees provides only weak corroboration, while a mobile phone provides stronger corroboration (although this is not always true globally; in some parts of the world, a mobile phone may be shared within a community).

The contextual information can be thought of as a different grade of authentication attributes in a continuum with canonical authentication attributes.

From a pragmatic viewpoint, using, for example, X.509 credentials that provide EPI (a "machine certificate") may approach the authentication strength of, for example, an X.509 software token (a "user certificate"). Both, after all, are based on the same cryptographic mechanisms. If a user is uniquely associated with a PC, and in a way that the user's identity is bound to the PC's and, thus, to the PC's X.509 credentials, and if it's not possible for another end user (rather than an administrator) to access and use the credentials without masquerading as the first user, then this approach provides a similar level of confidence as using a PIN-protected X.509 software token.

Conversely, X.509 software tokens are more like EPI than X.509 hardware tokens (such as smart cards). To what degree are they "held by only the user"? NIST SP 800-63-1 categorizes a "Multi-factor Software Cryptographic Token" as Level 3, whereas a "Multi-factor Hardware Cryptographic Token" is Level 4 (higher). However, if an X.509 software token is used on a PC in the enterprise's office that is accessible to all employees, then the only things someone needs to masquerade as the user are the user's PC password and token PIN, so the assurance level collapses to Level 2 or even Level 1. Some regulations do not accept X.509 or other software tokens as sufficiently strong — for example, the U.S. Drug Enforcement Administration's interim final rule for electronic prescriptions demands "a hard token stored separate from the computer being accessed."

Thus, the distinction between canonical authentication attributes and these additional, "ambient" authentication attributes is largely semantic. Just like counting factors, making this distinction doesn't tell us anything meaningful about the strength of an authentication method that incorporates them. Furthermore, we may speculate that a sufficiently large and varied set of ambient authentication attributes may provide an acceptable level of confidence, absent any canonical authentication attributes (this idea will be discussed in more detail in forthcoming Gartner research).

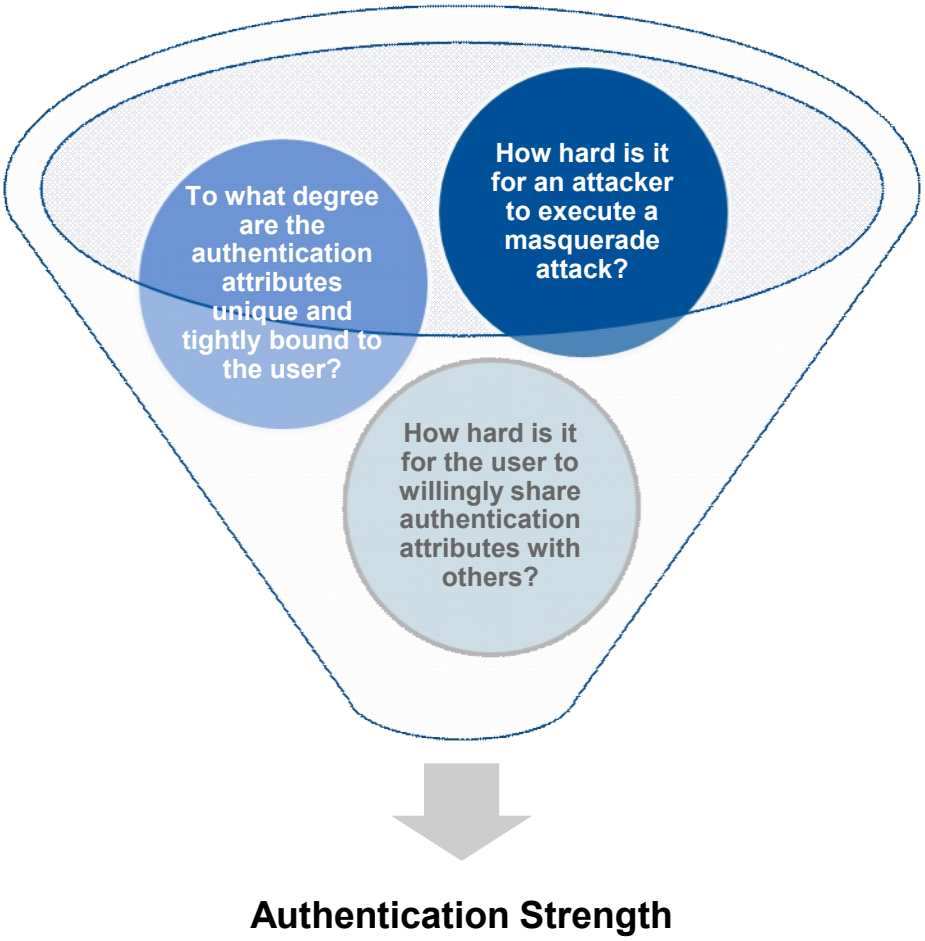
However, just like counting factors, the distinction may be one that's important to regulatory compliance.

If Counting Factors Isn't Enough, Then How Can We Evaluate Authentication Strength?

The hard truth is that we are forced to evaluate the strength of each distinct authentication method on its own terms. Currently, the industry lacks any transparent, formal methodology for this. (Although standards like NIST SP 800-63-1, "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, Draft 3" categorize some specified methods according to AL, the rationale behind this categorization isn't clear.) However, Gartner has created a simple framework for clients to carry out their own evaluations of candidate authentication methods (see "Gartner Authentication Method Evaluation Scorecards, 2011: Overview"). Figure 3, Figure 4 and Figure 5 sketch out our approach.

We take authentication strength to be a function of the "particularity" of an authentication method, its resistance to masquerade attacks and the difficulty of sharing authentication attributes (see Figure 3).

Figure 3. Authentication Strength Comes From a Combination of Three Things



Source: Gartner (September 2011)

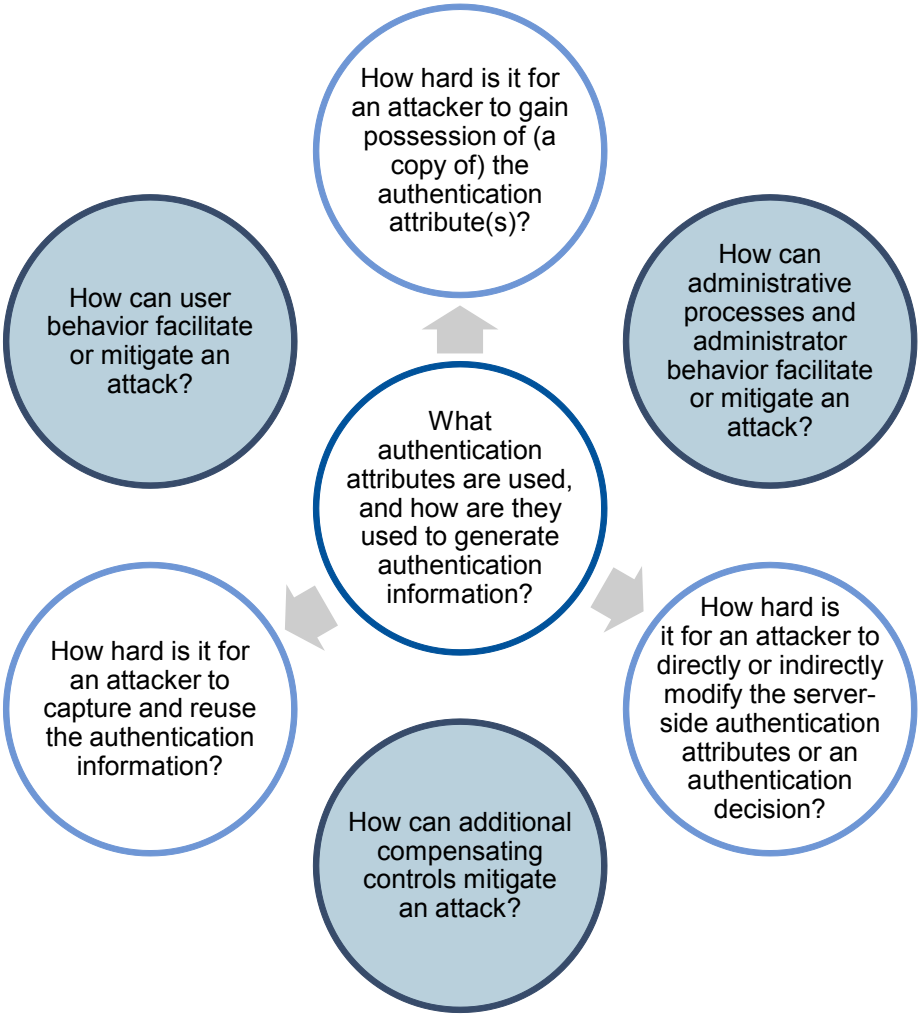
We note that a method's inherent or "raw" resistance to attack can be modified — strengthened or weakened — by external considerations that will vary from one implementation to another (see Figure 4).

Figure 4. People, Processes and Controls Modify the Raw Resistance to Masquerade Attack

Source: Gartner (September 2011)

At finer granularity (see Figure 5), to evaluate the raw resistance to masquerade attack (white), we "deconstruct" the method and consider the ways in which an attacker might obtain authentication attributes or authentication information, or subvert an authentication decision. To evaluate the effective resistance (blue), we also fold in the ways that user and administrator behavior, administrative processes and compensating controls can facilitate or mitigate an attack.

Figure 5. Evaluating Raw Versus Effective Resistance to Masquerade Attack



Source: Gartner (September 2011)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Market Guide for User Authentication"

"Market Guide for Online Fraud Detection"

"Transform User Authentication With a CARTA Approach to Identity Corroboration"

Note 1 Definition of "Authentication"

The definition we adopt here is based on a number of similar definitions from canonical industry standards. For example:

- To confirm a system entity's asserted principal identity with a specified or understood level of confidence ("Glossary for the OASIS Security Assertion Markup Language [SAML] V2.0").
- Entity authentication is the corroboration of the claimed identity of an entity and a set of its observed attributes ("Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management, Consultation Paper v2.01").
- The process of establishing confidence in the identity of users or information systems (NIST SP 800-63-2, "Electronic Authentication Guideline").

We use "corroborating" in preference to "confirming" or "verifying" because it better conveys the idea that authentication cannot provide absolute proof of a user's claimed identity.

Note 2 Authentication Method Types

The FIPS Pub 41 taxonomy was restated by the National Computer Security Center in NCSC-TG-017, "A Guide to Understanding Identification and Authentication in Trusted Systems," 1 September 1991. Here, an authentication method based on knowledge is called Type 1, a method based on what the user holds is Type 2, and a method based on an inherent characteristic is Type 3. All types may be described as "authentication by possession," although this is sometimes used to mean only Type 2.

The descriptions are often stated in the second person: "something you know," "something you have" and "something you are." However, only the first description is unambiguous and inclusive. Because it's common to call someone in possession of a (payment) card the cardholder, it seems natural to use the phrase "something held." A biometric characteristic can arguably be described as "something you have" or "something you possess," and behavioral biometric characteristics are as much "something you do" as "something you are." Thus, the language we use here to encompass all biometric characteristics is "something inherent."

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp