

FINANCIAL SERVICES TECHNOLOGY CONSORTIUM



BMA Working

PROJECT WORKING NOTES

Better Mutual Authentication Terminology

DRAFT version 0.4 as of September 21, 2006

© 2005 - 2006 FINANCIAL SERVICES TECHNOLOGY CONSORTIUM
ALL RIGHTS RESERVED

Better Mutual Authentication Terminology

Document Revision History

	Date	Author	Comments
0.1	Dec 21	C. Wade	Base document
0.2	Dec 26	C. Wade	Major updates
0.3	Jan 9	C. Wade	Major updates, first version circulated to entire Project
0.4	September 21	D. Schutzer	Major updates

1 Introduction

This document proposes a set of terms to be used in describing requirements for, and approaches to achieving, *better mutual authentication* in a retail financial services context. In particular, terminology is an integral part of *architecture*, and this document should be treated as an adjunct to the BMA Architecture document.

The definitions provided here are intended to provide sufficient explanations of the underlying concepts to serve as a useful reference for BMA Project Participants. Furthermore, the terminology definitions incorporate extensive cross-references to related terms in order to facilitate improved understanding of how these terms should be used in practice.

There are many existing terminology compendia that address security terms, some even focused on financial applications or on authentication issues. The primary reason for introducing a BMA terminology document is not to duplicate those other efforts, but to highlight the way in which the BMA Project uses specific terms so that BMA output documents can be properly understood by all readers. A secondary reason is to clarify terms that are not used consistently in the broader literature, or where there are conflicting definitions.

In defining terms, there has been a bias to remain as close as possible to traditional English language definitions, and a variety of dictionary sources have been used. There are also existing American National Standards (and to a lesser extent ISO and NIST standards) that include normative definitions of some of the terms defined in this document. The intent is that definitions in this document should supersede those “standard” definitions.

Reference sources will be cited in a bibliography that will be added to a subsequent version of this document

2 Recommended Terminology

Working definitions are presented below for key terms. As much as possible, definitions presented here are based on common dictionary references, but have been adapted to the authentication problem space within a retail financial context.

2.1 Access Control

Access control, simply stated, is a procedure used to determine if a party should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

Access control is often expressed in terms of negatives. For example, ISO 7498-2 defines access control as “the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.”

However, there are many circumstances where it may be more effective to describe

Better Mutual Authentication Terminology

access control in positive terms – *i.e.*, what is allowed in the way of authorized use of a resource. Positive expressions are most effective when the general policy is to “disallow everything except what is expressly allowed” – a policy approach that is appropriate for financial services.

Access control services are often characterized in terms of the *granularity* of control provided. *Coarse* control applies to situations where access is granted on an “all or nothing” basis, whereas *fine* control describes an approach that allows localized decisions about which specific resources a party is, or is not, allowed to access or use. Within a financial services context, the specific application determines what granularity of access control is required.

Authentication (see definition at 2.5 below) is an inherent sub-procedure within an *access control* procedure, as it is necessary to authenticate the party requesting access. However, access control should not be confused with authentication. In particular, access control is typically used to determine what a particular, authenticated party is allowed to do, or not do.

2.2 Account Number

This is simply a *name* (see 2.29 below) of a financial account – *e.g.*, DDA¹, credit card, loan, mortgage, retirement, trading, or investment. If presented as a *claim* (see 2.15 below) during authentication, then the account number is used as a shorthand expression to claim rights and privileges to access information about the account, or to conduct transactions against the account.

2.3 Assurance Levels

This relates to the confidence that the authentication process is correct. For example an Authentication Assurance Level is subjectively related to the strength of the authentication (likelihood of false rejects, false accepts or successful spoofing). For example, NIST developed for OMB, 4 authentication assurance levels. Level 1 – Little or None, is sometimes associated with requiring no authentication, not even ID and password. Level 2 – Some is sometimes associated with a single factor authentication, such as ID and password. Level 3 – High, is sometimes associated with 2 factor authentication, such as ID and Password and a hardware token (something you possess). Level 4 – Very High, is sometimes associated with 3 factor authentication, such as something you know, something you possess, something you are.

2.4 Attribute

A subject is an entity represented or existing in the digital realm which is being described or dealt with. Every subject has a finite number of identity attributes. A subject can be human or non-human. Non-human examples include:

¹ Demand Deposit Account. For retail banking, the DDA is what most consumers think of as their “checking account.”

Better Mutual Authentication Terminology

- Devices and computers
- Digital resources
- Policies and relationships between other subjects.

Identity attributes exist within the context of ontologies. A simple example of an ontology is “A cat is a kind of animal” An entity represented in this ontology as a “cat” is therefore invariably also considered to be an “animal.” In establishing the contextual relationship of identity attributes to one another, ontologies are able to represent identity in terms of pre-defined structures. This in turn allows computer applications to process identity attributes in a reliable and useful manner.

For humans, some examples of identity attributes are name, address, phone number, color hair, social security number, height, weight, and so on.

2.5 Authentication

In normal usage, *authentication* refers to a *procedure* that is typically performed within the context of a larger system (see definition of Authentication System, at 2.8 below)

The following definitions reflect usage expressed in popular dictionaries:

- **authenticate:** to confirm or establish the authenticity of some claim or some thing
- **authenticity:** confirmable or verifiable truth; the legality (legal validity) of a claim or agreement

By direct implication, an “authentication procedure” must receive a claim from some party (the *claimant*), and provide some assessment of the authenticity of the claim.

The *result* of authentication (see definition at 2.7 below) is an assessment of confidence that the claim is, or is not, valid. What is essential is that the claim be something that *can* be confirmed to some acceptable level of confidence using *available* means.² The means by which claims are confirmed involves one or more tests based on verifiable conditions or information objects – referred to here as *authenticifiers* (see definition at 2.9 below) – that can be directly associated with the claim.

An authentication *claim* is a statement or proposition that, depending on context and circumstances, is presented either explicitly or implicitly. Claimants are typically

² There is often misunderstanding about the nature of claims used within practical online authentication procedures. In particular, a claim of *identity* cannot easily be confirmed as true or false in an online context. While it may be common to use terms like *identification* or *identity*, in most cases true identity is not relevant, nor is it practical to test claims of identity.

asserting that they have certain rights, privileges, entitlements, or authorizations. *Authority* may also be the subject of a claim.

For example, when a computer user enters a “userid,” the user is making the claim that he or she is authorized to whatever rights or entitlements have been granted to the party (or parties) associated with the userid (usually determined by some lookup process involving a database or directory). Another way of putting this is to observe that the user is really making a claim to be authorized to act in a certain capacity or role. Such claims have nothing to do with the true identity of the user – after all, a userid is nothing more than a *name* (see 2.29 below), as are things like SSNs and *account* numbers.

Within retail financial services, authentication is almost always associated with *access control* (ref. 2.1 above) or *authorization* (ref. 2.11 below). Claims are usually expressed by reference to an account number (2.2), but may also be expressed in terms of common names or widely recognized unique identifiers, especially taxpayer numbers (*e.g.*, SSN).

Retail financial services also require *mutual* authentication, where each party authenticates the other as part of access control or for authorization of transactions (ref. *Mutual Authentication*, 2.27 below).

2.6 Authentication Device

The term, *authentication device*, is used to refer generically to any form of device that can be used in performing authentication, either by the claimant, or the authenticating party, or both. Some common examples of authentication devices include:

- “Scratch” card (passive)
- “Bingo” card (passive)
- Mag stripe card (passive)
- One-Time Password fob
- Smart card
- SIM card
- Crypto token
- USB dongle
- Trusted Platform Module (TPM)
- Biometric scanner

Authentication devices may be either *passive* or *active*. The first three “cards” cited above are examples of passive devices, since they perform no processing, and merely serve as storage devices for information objects. The other examples are all active, and perform some sort of operation on *authenticifiers* (see definition at 2.9 below) stored within the device, or scanned using the device.

Active authentication devices generally include a secure storage mechanism, or *vault* (see 2.40 below). Depending on the device capabilities and vault storage capacity, a single authentication device may be able to support multiple authenticifiers, possibly including credentials (2.18), such as digital certificates (2.19).

2.7 Authentication Result

Since authentication is often a sub-procedure used in other security procedures or services, it must produce some *result* that can be used to determine if a presented claim should be accepted. Traditionally, authentication results are binary – either positive if the claim is accepted, or negative if the claim is rejected.

While not typical in current practice, it would be more effective if authentication results were presented as a multi-level, or even continuous, expression of *confidence* in the authenticity of presented claims. As an example, a fine-grained access control system could use a confidence result from an authentication procedure to determine whether or not to allow access to a specific resource based on an overall risk assessment, where authentication confidence would be one factor in assessing risk on a dynamic basis.

It is worth noting that all authentication systems have some probability of error for positive results – so-called “false positives” – and a different error probability for negative results – “false negatives.” In other words the ratio of false positives to true positives is not necessarily related to the ratio of false negatives to true negatives. If the rates of false positives and false negatives can be determined for some authentication process, then this information can be used to further qualify the veracity of authentication results.

2.8 Authentication System

In the real world, *authentication procedures* (see 2.5 above) depend on a variety of services used to establish preconditions, including the ability to recognize claims and to associate each claim with a set of *authenticifiers* (ref. 2.9 below) or *credentials* (ref. 2.18 below) that can be used to test the authenticity of claims. Procedures must be in place to enroll claimants, associate credentials with claims, manage credentials, and resolve problems. Typically, authentication procedures will rely on databases or directories built and maintained by other processes. In total, these processes comprise an *authentication system*.

The overall veracity and effectiveness of authentication is determined as much by the authentication system as by the actual authentication procedures and techniques employed – *an authentication system is only as strong as its weakest link*. For example, if a credential is issued to the wrong party (potentially, an impostor), then any authentication procedure using that credential will consistently authenticate the wrong party.

Authentication systems also depend on governing policies, management practices, and operational procedures. Even the best authentication system poorly managed or badly operated will yield low quality results, while sound practices and policies can

compensate for technical deficiencies in an authentication system. And, of course, inappropriate policies will generally produce unintended consequences.

2.9 Authenticifier

An *authenticator*³ is an information object or condition that can be evaluated in order to confirm the veracity of an authentication *claim*. Some examples of common *authenticifiers* include:

- Shared secrets, including passwords and keys used to generate one-time passwords
- Asymmetric cryptographic keys
- Physical metrics, including biometrics
- Access to a common resource, including use of alternative channels such as telephone circuits
- Shared knowledge – *e.g.*, challenge question to claimant with associated response
- Contextual clues – *e.g.*, characteristics of the computer or network connection used by a claimant, including dynamic conditions
- Behavioral patterns

In general, an *authenticator* must be associated with a specific claim. However, there are a variety of schemes for making such associations and maintaining the association of claim to authenticifier throughout a life cycle.

One way that claims are bound to authenticifiers is through use of a *credential* (see 2.18 below). However, it is important to avoid confusing authenticifiers with credentials. In particular, while every credential refers to at least one authenticifier, an authenticifier need not be associated with a credential.

For example, an asymmetric key pair can be used as an authenticifier, where the claimant holds the private key and an authenticating party has access to the corresponding public key. A credential, in the form of a digital certificate, might serve to bind the public key to the claimant (or the claim). During authentication, the claimant can be presented with a challenge that is cryptographically processed with the claimant's private key to produce a response that can subsequently be tested using the public key contained in the digital certificate. Note that, in this example, the authenticating party need *not* depend on a digital certificate, but could use some other means to associate the appropriate public key with the claim.

³ "Authenticator" is not a word in the English language (though it is a French word). It is being introduced here as a more convenient term than some of the compound phrases, such as "authentication information," that are sometimes used in security literature. The NAS/NRC "Who Goes There" report suggests "authenticator" as an equivalent term, but this can also mean "one who authenticates." Another reason for introducing "authenticator" is to explicitly avoid misuse of terms, such as "token," or "credential" that have taken on confusing semantic baggage.

Better Mutual Authentication Terminology

As another example, a password is an authenticator in the form of a shared secret. During authentication, a claim is expressed as a userid or login ID, and the claimant is then asked to present the shared secret password. If the password matches what the authenticating party has on file, then there is positive evidence to support the claim. Passwords are normally stored in some directory or database that is indexed by a claimant's userid. While the record in such a database containing the userid and password for a particular claimant could arguably be considered a *credential*, this is not a common use of the term.

In some cases, authenticators can be mapped to *authentication factors* (see Multi-factor Authentication at 2.28 below). However, the concept of multi-factor authentication is predicated on use of independent verification procedures or tests, whereas an authenticator is simply something that can be tested.

The term, *token*, is often used in a manner synonymous with *authenticator*, although the meaning of token has always been narrower than the definition provided here for authenticator. Recently, *token* has taken on a broader definition that even includes passwords,⁴ though this is not yet widely acknowledged. Originally, tokens were considered to be physical devices or things like mag stripe cards that could be used in authentication. Later, the concept was extended to include “soft” tokens, and, in some recent documents, shared secrets like passwords. None of these uses of the term, token, relate well to accepted English language definitions.

2.10 Authority

An authentication authority is a person or organization that attest to the identity of an entity (some set of identity attributes), usually with a signed Digital Certificate or a Security Assertion Mark-up Language (SAML). See Certificate Authority.

2.11 Authorization

Authorization is a grant, by some *authority*, of permission to take some action or perform a transaction. Implicit in this definition is the concept that the *authority* must be *authenticated*. Furthermore, the *authorization* must provide some proof that the authenticated authority granted specific permissions or transactions.

In traditional paper-based transactions, an authority applies a wet ink signature to the document that grants permission—*e.g.*, a paper check is signed by the account holder (the authority) to authorize payment of a specific amount to the indicated payee.

Electronic documents or transactions can be digitally signed using techniques that allow any recipient of the signature to authenticate the source authority, and also to confirm that the signed document or transaction presented is the same as what the authority actually signed (integrity proof). While digital signatures are not the same as wet ink signatures, they can play a similar role in providing authorization.

⁴ For example, NIST 800-63 defines a password as one type of token.

Authorization in an electronic context can also be achieved by employing access control procedures (see 2.1 above). If a “button” to authorize a transaction can only be accessed by an authenticated authority, then pressing the authorize button can be construed as *authorization*. However, in a financial context, such an authorization procedure must provide accurate records indicating which authority initiated the transaction, along with the details of the specific transaction. Typically, policies will dictate that the authorizing authority be sent some sort of written confirmation of the transaction details.

An example of authorization via access control is an online banking bill payment application. If access to online banking services for a specific bank account is restricted to just the parties that can successfully authenticate as a designated account holder, then only an account holder will be able to click on a button authorizing payment of a specific bill. A record of the transaction will be entered into the transcript for the bank account, and confirmation will be provided in a statement provided to the account holder. Note that a fine-grained access control system could require further authentication of the party claiming to be an authorized account holder before the authorization “button” is presented. This might be based on some form of dynamic risk assessment.

2.12 Biometric

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for [authentication](#) purposes

2.13 Certificate

See *digital certificate*, 2.20 below.

2.14 Certificate Authority

A **certificate authority** or **certification authority (CA)** is an entity which issues digital [certificates](#) for use by other parties. It is an example of a [trusted third party](#). CA's are characteristic of many [public key infrastructure](#) (PKI) schemes.

There are many commercial CAs that charge for their services. Institutions and governments may have their own CAs, and there are free CAs.

2.15 Claim

Within the context of *authentication*, a party (or entity) presents a *claim* that will be tested for authenticity as part of an authentication procedure (see definition of *authentication* at 2.5 above). Typically, a claim is presented in the form of a *name* (see 2.29 below) that indirectly references whatever rights or entitlements are associated

Better Mutual Authentication Terminology

with the claim — *i.e.*, the *name* is a shorthand means of referencing a *claim* that may involve many parameters or attributes.

However, in some cases, claims to privileges or entitlements are stated directly within an authentication process. For example, when enrolling for authenticifiers (ref. 2.9 above) or credentials (ref. 2.18 below) to be used in subsequent authentication procedures, the claim may need to state what privileges or entitlements are to be associated with the credential.

2.16 Claimant

Within the context of *authentication*, the party (or entity) that presents a *claim* (see 2.15 above) to be authenticated is referred to as a *claimant*. A claimant may be a true person, or an insentient system or service. It doesn't really matter who, or what, a claimant is, only that it is the presenter of the claim.

In retail financial services, a customer seeking access to a financial service for a specific account is a claimant, but so is the financial service itself. The customer is claiming the rights, privileges or entitlements associated with their account, while the financial service is claiming to be the legitimate provider of services associated with the customer's account.

2.17 Confidentiality

Confidentiality has been defined by the International Organization for Standardization (ISO) as “ensuring that information is accessible only to those authorized to have access” and is one of the cornerstones of Information Security. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography.

2.18 Credential

While the term *credential* is widely used within the literature of security services — especially in relation to *authentication* — it is unfortunately not used in a consistent manner. Further complicating matters, the English language definition of *credential* is often inconsistent with use of this term within security literature.⁵

Credentials are authoritative statements or documents that associate *claims* with *authenticifiers*. An example of a widely used credential is a *drivers' license*, which actually binds multiple claims to multiple authenticifiers. A drivers' license can be used to confirm a claim of permission to drive an automobile, or a claim of age, name, or address. Every driver's license is issued by a state authority (*e.g.*, Registry of Motor Vehicles), and carries a seal and typically some difficult-to-forge mark of the authority (*e.g.*, a holographic image). A photograph of the claimant embedded in a drivers' license is one authenticifier that can be used to test claims. The physical

⁵ For additional commentary on problems with use of “credential” in security literature, see R. Shirey, “Internet Security Glossary,” <<http://www.ietf.org/internet-drafts/draft-shirey-secgloss-v2-02.txt>>.

drivers' license card can also be an authenticator, if the claimant presents it to the authenticating party.

In *multi-factor authentication* (see 2.28 below), credentials may also be associated with one of the three traditional “factors” – *something you know, you have, or about you* (SYK, SYH, SYA). However, it is awkward to say that a *credential* is a *factor*, due to inconsistent usage of both terms within the literature.

When a credential is tightly bound to a physical device in a manner that makes it difficult to duplicate (or forge) the credential, then the device plus credential may satisfy the criteria for a “something you have” authentication factor. For example, a “smart chip” that performs asymmetric cryptographic operations on securely stored private keys (authenticators) and also maintains copies of associated digital certificates (credentials) can be an effective way to satisfy the requirements for a SYH factor, since it represents a complete packaging of authenticators and credentials in a relatively secure device.

2.19 Delegation

Delegation is the act of giving power, responsibility or authority to someone (or something). When we talk about delegation in the context of administering computers and networks, we can be talking about either the Delegation of administrative authority (also called delegation of control); or the Delegation of authentication (allowing a service to use a user or computer account for access to resources)

2.20 Digital Certificate

A *digital certificate* (ref. 2.20 above) is an example of a *credential* suitable for use in an online context. A *certificate authority* (ref. 2.14 above) issues a digital certificate as a digitally signed document that contains names and attributes associated with the claimant, along with a public key to be used as an *authenticator* in testing subsequent claims. The digitally signed certificate binds the public key authenticator to claims that may be made by the certificate subject (claimant). However, use of asymmetric (private/public) keys as authenticators in authentication does not require use of digital certificates.

2.21 Digital Identity

See Identity

2.22 Directory

(1) An organizational unit, or container, used to organize [folders](#) and [files](#) into a [hierarchical](#) structure. Directories contain [bookkeeping](#) information about files that are, figuratively speaking, beneath them in the hierarchy. You can think of a directory as a file cabinet that contains folders that contain files. Many [graphical user interfaces](#) use the term [folder](#) instead of *directory*.

[Computer](#) manuals often describe directories and file structures in terms of an [inverted tree](#). The files and directories at any level are contained in the directory above them. To [access](#) a file, you may need to specify the [names](#) of all the directories above it. You do this by specifying a [path](#).

The topmost directory in any [file](#) is called the [root directory](#). A directory that is below another directory is called a [subdirectory](#). A directory above a subdirectory is called the [parent directory](#). Under DOS and [Windows](#), the root directory is a back slash (\).

To [read](#) information from, or [write](#) information into, a directory, you must use an [operating system command](#). You cannot directly edit directory files. For example, the DIR command in [DOS](#) reads a directory file and displays its contents.

(2) In [networks](#), a [database](#) of [network](#) resources, such as [e-mail](#) addresses. See under [directory service](#).

2.23 Enrollment

Enrollment is a procedure that records in some list, directory, or database additional attributes, entitlements, or credentials to be associated with a previously registered party or a party for which an established relationship already exists. An enrollment procedure typically considers the qualifications of the enrolling party, and whether the additional attributes are appropriate, or if requested entitlements should be granted.

Enrollment is often used to *bind* a known entity's *name* to specified *attributes*, *entitlements*, or *credentials*—or even other *names*.

De-enrollment (or unbinding) is a related procedure that removes or deletes previously enrolled attributes, credentials, or entitlements.⁶

Credential establishment or issuance is a special case of enrollment that plays a major role within *authentication systems* (ref. 2.8 above). Before a party can be authenticated, they must implicitly or explicitly enroll credentials that will be used in confirming subsequent authentication claims. In this case, enrollment binds a credential to a specific party or claim.

2.24 Entitlement (privileges, rights)

Entitlement refers to being granted rights to access and modify information and resources, such as financial data, confidential records, web services and programs. Access control is a critical component of security and compliance efforts, and involves managing who has what rights, based upon authentication of the user.

⁶ One distinction between enrollment and registration is that registration is not easily reversed. In many situations, only de-enrollment procedures are provided.

2.25 Integrity

Integrity here refers to the integrity of information – that is unaltered, in its original state.

2.26 Interoperability

The ability of software and hardware on different machines from different vendors to share [data](#); to exchange or use information.

2.27 Mutual Authentication

The following is the definition of *mutual authentication* developed at the BMA Boston meeting on December 8, 2005. Several alternative wordings are provided based on comments received in subsequent discussions.

“Mutual Authentication” refers to the process whereby an FI’s customer and a financial services application exchanging [[message traffic](#) | [information](#)] each obtains sufficient assurance that the other party is authentic, and that the [[message stream](#) | [information exchange](#)] has integrity, and that no other parties are able to participate in the information exchange.

The level of assurance shall be appropriate to the risk associated with the interaction.

2.28 Multi-factor Authentication

Authentication that determines authenticity of claims by employing multiple, independent factors is termed *multi-factor authentication*. A *factor*⁷ is something that can contribute to an authentication result, usually in a manner designed to reduce false positives or false negatives.

Traditionally, three types of factors have been considered independent enough to increase confidence in authentication results for claims made by persons:

1. Something You Know (SYK) – A shared secret known by a person; typically a password or PIN
2. Something You Have (SYH) – A physical thing held by the person being authenticated, and presumably difficult to forge or duplicate
3. Something You Are (SYA) – A physical or biological characteristic of the person; often referred to as a “biometric”

In the traditional definition of multi-factor authentication, there must be two or more combinations of these three factors, but only one of each type of factor – *i.e.*

⁷ Within the context of authentication, the term, “factor,” is seldom used outside of the definition of multi-factor authentication.

Better Mutual Authentication Terminology

SYK+SYH, or SYK+SYA, or SYH+SYA, or SYK+SYH+SYA. The rationale for this restriction is that authentication results can only be improved when tests are conducted against independent factors, since multiple tests against a single type of factor would generally be vulnerable to any compromise affecting the factor.

While the traditional concepts behind multi-factor authentication are sound, there are several problems worth noting. First, this terminology is oriented toward authenticating persons, not systems or services. Second, the three types of factors cited are not well defined in current literature. Third, some potentially useful tests are not addressed by these three types of factors (especially, contextual clues). And fourth, while independence of factors promotes greater confidence in authentication results, it may be possible to utilize authentication tests that improve confidence in results, even though the tests represent only one type of factor.

For retail financial services, multi-factor authentication is defined as any authentication process that employs multiple independent tests specifically designed to substantially improve confidence in authentication results – *i.e.*, significant reductions in false positives and false negatives. Furthermore, in the case of authenticating human customers of financial services, multi-factor authentication must involve at least two tests where one test does not depend on human recall of shared secrets.

This definition is not limited to authentication of persons, and should apply to authentication of systems as well.

2.29 Name

Within the context of electronic *authentication systems*, the *names* associated with various parties, entities, and resources are of critical importance. *Claims* (see 2.15 above) are often expressed indirectly via a *name* that maps to the claim being made. For example, a financial institution may claim to its customer that it is the legitimate provider of financial services in an online context by presenting a domain name or URL (both names) during a web-based interaction. Similarly, a customer may provide their account number (a name) as a shorthand expression of the claim that they are the party authorized to access account information or conduct transactions involving the account.

In modern systems, there are many types of names that can be used to refer to an entity or as a shorthand reference to a claim, often with substantial overlap. For example, a consumer may be known by their common name, taxpayer number, drivers' license number, employee number, mailing address, email address, telephone number, financial account number, or some userid assigned to them for the purpose of authentication or access control. Similarly, the plethora of names consumers must use to reference their financial institutions is a source of potential confusion, especially as financial institution names change on a frequent basis due to system updates or mergers/acquisitions.

Names are useful only when *directory* services (see 2.22 above) exist to map names to other names or attributes. For example, the Internet's DNS service is used to map

domain names (moderately useful to people) into numeric IP addresses (less people-friendly), often on a dynamic basis. Confidence in *authentication results* (ref. 2.7 above) is often directly related to confidence in the meaning (semantics) of a name, or confidence in some directory service used to map a name to attributes or another more meaningful name.

2.30 One-Time Password (OTP)

An OTP (one-time password) system generates a series of passwords that are used to log on to a specific system. Once one of the passwords is used, it cannot be used again. The logon system will always expect a new one-time password at the next logon. This is done by decrementing a sequence number. Therefore, the possibility of replay attacks is eliminated.

The series of passwords is created by the client, which combines a *seed* value with a secret password that only the client knows. This combination is then run through either the MD4 or MD5 hash functions repeatedly to generate the sequence of passwords.

Smart cards and token-based authentication methods use one time passwords. The IETF has developed an OTP that is based on the earlier Bellcore S/KEY one-time password system. A number of Internet RFCs discuss one-time passwords. These include [RFC 1760](#) (The S/KEY One-Time Password System, February 1995), [RFC 2243](#) (OTP Extended Responses, November 1997), [RFC 2289](#) (A One-Time Password System, February 1998), and [RFC 2444](#) (The One-Time- Password SASL Mechanism, October 1998). Also see [RFC 1511](#) (Common Authentication Technology Overview, September 1993), [RFC 1704](#) (On Internet Authentication, October 1994), and [RFC 2401](#) (Security Architecture for the Internet Protocol, November 1998).

2.31 Privacy

Data privacy refers to the evolving relationship between technology and the legal right to, or public [expectation of privacy](#) in the collection and sharing of [data](#).

Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information
- Criminal justice
- Financial information
- Genetic information

The challenge in data privacy is to share data while protecting the personally identifiable information. Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared.

2.32 Registration or Relationship Establishment

Registration is a process used to establish a *relationship* between two or more parties. Registration is accomplished by recording in some authoritative list (or directory) references to entities that are of a specific type, meet certain requirements, or have appropriate qualifications or entitlements. A *registrar* is the *authority* that determines whether or not an entity may be registered in a particular list or directory, while the *registrant* is the entity to be registered. Registration establishes a *relationship* between the registrant and registrar.

Implicit in any registration process is that any entity presented for registration will be evaluated for suitability, acceptability or compliance with stated conditions.

Registration associates a *name* with each registered entity. Typically, names are unique within each registration context, and names may even be assigned during the registration process.

In the financial industry, *customer registration* is often associated with “account opening,” which implicitly includes an *enrollment* procedure for the customer’s first account.

2.33 Registrar

The entity that provides registration

2.34 Registry

A user registry holds user account information, such as a user ID and password, or digital certificates that can be accessed during authentication.

2.35 Relationship

Before parties can authenticate each other, some sort of *relationship* must first be established. Relationships can be formal or informal in nature. Formal relationships are often established via some sort of contract or agreement between the parties, and may be subject to policies established by authorities, such as legislatures, regulatory bodies, or industry rule-making associations.

Within a retail financial context, the relationships between financial service providers and consumers are governed by a broad array of existing laws, regulations, industry rules and standard contractual agreements that dictate the responsibilities of both parties. In particular, financial institutions must comply with

“Know Your Customer” (KYC) regulations that stipulate what due diligence is required in determining that the customer is who they claim to be, and not an imposter acting as another real or fictitious person.

2.36 Re-usability (of authentication devices, authenticifiers, credentials)

The ability for a user to use the same authentication device (such as a OTP token) with than one service

2.37 Role

In a role-based authentication software system, users are assigned one or more predefined roles. These roles then determine the user's privileges; the information they can see, areas they can access, and items they are able to change

2.38 Single Sign-On (SSO)

Single sign-on (SSO) is a specialized form of [software authentication](#) that enables a user to authenticate once and gain access to the resources of multiple software systems

2.39 Validate

Shirey⁸ defines *validate* as follows:

1. Establish the soundness or correctness of a construct. Example: certificate validation.
2. To officially approve something, sometimes in relation to a standard. Example: NIST validates cryptographic modules for conformance with FIPS PUB 140 [FP140].

The first definition is most relevant to the BMA topic, and includes any process that aims to establish that data relationships are properly maintained, or that data structural rules have not been violated. Since *validation* merely determines that a construct is correct, it is a weaker statement than *verifying* some claim (see 2.41 below). However, validation is often a necessary process in authentication, and may be associated with “controls” used to audit compliance with stated practices.

2.40 Vault

A *vault*, within the context of authentication, is a secure storage facility for *authentifiers*, and possibly *credentials*. A vault may be a software construct, such as an encrypted file or database, or it may be a special-purpose hardware module designed to protect authentication information. Vaults are often associated with

⁸ R. Shirey, “Internet Security Glossary,”
<<http://www.ietf.org/internet-drafts/draft-shirey-secgloss-v2-02.txt>>.

Better Mutual Authentication Terminology

cryptographic processing modules designed to encrypt data stored in a vault, or to perform cryptographic operations on keys maintained in a vault so that these keys do not have to ever leave the vault “in the clear.”

Software vaults are commonly used to store passwords, and are available as standalone applications. They also come built into web browsers and some other applications, and may come as an embedded module within a modern PC operating system. Software vaults also store symmetric (secret) and asymmetric (private) keys.

Nearly all *authentication devices* (see 2.6 above) include some sort of vault, often built into a multi-purpose crypto chip (a.k.a., smart chip). Depending on the capabilities of a particular authentication device, the embedded vault may support multiple authenticifiers, potentially of different types. The vault may be designed to prevent any form of access to its contents, except through indirect cryptographic operations, and may even be designed to destroy stored keys in the event of tampering or attempts to physically override data protection mechanisms.

A potential benefit of having vaults associated with authentication devices is that multiple authenticifiers can be maintained on one device. This leads to the potential that multiple parties might rely on one authentication device, but each relying party could associate its own authenticifier (and perhaps credential) with the claimant that possesses the authentication device.

It is worth noting that some *vaults* implement *access controls* to prevent unauthorized access to authenticifiers. This leads to a bit of a recursion within authentication systems, since the vault must authenticate all attempts to access its contents. Typically, this is done through some sort of PIN, but increasingly vaults are accessed using biometric scans.

2.41 Verify

Shirey⁸ defines *verify* as follows:

To test or prove the truth or accuracy of a fact or value.

In the BMA context, *claims* are *verified* during an authentication procedure – *i.e.*, verification is an assessment of the authenticity of a claim.

3 Other Terms

The terms in this section may be used within BMA documents, but some caution is urged as these terms tend to have confused meanings, or are frequently misused.

3.1 Authentication Factor

3.2 Federated Identity

3.3 Identification

3.4 Identity

3.5 Identity verification

3.6 Pharming

3.7 Phishing

3.8 Phraud

3.9 Risk-based Authentication

3.10 Token

3.11 Trust (trustworthy)

3.12 Victim

4 Terms to avoid

These terms are so overloaded or confusing in their popular usage that they should be avoided within BMA documents.

4.1 Account hijacking

4.2 Identity theft

4.3 Identity management