Identity Management

IDSEC

May 13, 2016

Providing the Transition
from Communication Security
to Information Security

Table of Contents

SECTION **PAGE**

Section 1 Identity Security Preface 5

Identity Elements 7

ID/Password/PIN 7

Biometric 8

Electronic Signature 9

GEO Location 10

Machine Identification 10

Vertical Market Identifiers 11

e-Profile 11

Token 11

Trust and Liability 13

Authentication 15

Authorization 15

Revocation 15

Access Control 17

Identity Security Controls 18

Persistent Protection of Data 19

Options for an Identity Security 20

Section 2 Distributive Ledger and Blockchain in Security Preface 22

Introduction 22

Blockchain as a Secure Envelope with Identity and Encryption Enforcement 24

Securing Blocks of Financial Data 24

Blockchain as a Crypto Process for Differential Access 27

A Blockchain Encryption Framework 28

Permissions as Enforcement Attributes 30

Copyright 2016
All Rights Reserved

Attribute Listing for Financial Services Components....31
Background Material Associated with Financial Services Components and Attributes...31
A Secure Packet Based on a CKM Header and Linkage to Transaction Details....32
Section Three Blockchain Usages Introduction....34
A Sample Object Oriented Secure Blockchain and Distributive Ledger Architecture....35
Building a Secure Transaction Model....36
Details of a Secure Blockchain Distributive Ledger Use Case....40
A Secure Cloud Environment....40
A Sample Online Cloud Access Control Use Case Enforced by Encryption....41
Secure Payment Transaction Process....44
Overview of an Information Collaboration Model....44
Annex A. Setting the Security Stage....53
Annex B. Defining Objects for a Currency....57

List of Figures

FIGURE **PAGE**

Figure 1 Identity, Authentication and Authorization....7
Figure 2 Identity Elements....13
Figure 3 Blockchain Model....24
Figure 4 Secure Transport Envelope....25
Figure 5 Purchase Order Transaction Envelope....25
Figure 6 Differential Access on a Finance Report....27
Figure 7 Payment Voucher....28
Figure 8 Persistent Enforcement with CKM Encryption....29
Figure 9 Financial Service Components in the Blockchain....30
Figure 10 Blockchain Packet Flow....33
Figure 11 Distributive Ledger....37
Figure 12 Information Collaboration Model....41

Copyright 2016
All Rights Reserved

Figure 13 Unencrypted Data Moving Through a Financial System 46
Figure 14 Bank Start-Up of Information Collaboration Model 47
Figure 15 Establish Supplier Online Information Collaboration Model 48
Figure 16 Establish Bank Customer Information Collaboration Model Client 49
Figure 17 Order Placement 50
Figure 18 Process Cart Using Secure Financial Protocol 51
Figure 19 Process Payment – Bank to Bank Transfer 52
Figure 20 Enterprise Security Categories 53
Figure 21 End to End Security Infrastructure 55
Figure 23 Objects within a Financial Instrument 60
Figure 24 Objects for Handling Currency 61
Figure 25 Identifying Features of the Dollar Bill 62

List of Tables

TABLE PAGE

Table 1 Financial Service Components 31
Table 2 Financial Service Component and Access Permissions 32
Table 3 Attribute Labeling 42

Copyright 2016
All Rights Reserved

Section 1 Identity Security Preface

Globalization of businesses and the increasing integration of information technologies are compounded to make diversity of identity management a potential obstacle to the continuing development of the enterprise's objectives. To address this, there is a requirement for an integrated approach to identity management to automate, accelerate, and simplify identity creation and maintenance. In a broad context, identity management can be referenced as Identity Security or IDSEC for abbreviation.

Identity Security is a convergence of technologies and business processes. This convergence has drivers from both the business and technology perspective to:

- Enable a higher level of e-business by accelerating movement to a consistent set of identity management standards
- Reduce the complexity of integrating business applications
- Manage the flow of users entering, using, and leaving the organization
- Support global approaches/schemas for certain categories of operational tasks
- Respond to the pressure from the growing numbers of Web-based business applications that need more integration for activities such as single sign-on.

Establishment of Identity can be a difficult process. Identity is what makes something or someone the same today as it, she, or he was yesterday. Importantly, identity can refer to a thing (e.g., a machine) as well as a person. Identity is, normally, a global event (i.e. Don is always Don). Things and people can have different identities when working with different systems, or can have more than one identity when working with a single system, perhaps when working in different roles.

A typical large enterprise is operated by people who join as staff (permanent or temporary), contractors, and business partners. These people are assigned roles and act in them. Roles can also be performed by machines. It is possible to define roles as associations to various access models such as physical access, logical access, functional access, or access to content. These roles are always "temporary" in the sense that they have no fixed duration. Eventually people or machines either change roles or leave, creating a need for identity information to be actively managed and maintained throughout its lifecycle, frequently across multiple systems. Roles are, normally, a local event, under the control of the owner of the system or information being processed by that system.

So, identity security can consist of a define set of identity elements and roles. But, for identity security to be affective as a security tool there must be trust or a high assurance that the identity components of identity elements, encryption, and protocol are themselves protected.

Trust also can have another definition beyond protection. Trust can be aligned with liability. Trust is something we understand at a human level, but not necessarily when it comes to business-to-business relationships or to the technical systems needed to support business

Copyright 2016
All Rights Reserved

relationships. Trust can get translated into the notion of authority, where authority originates, and how it gets delegated. Liability is a business concept that can be objectively measured, and since it is often used in making business decisions. As a defined relationship between trust and liability evolves, another step takes place once a relationship can be established between trust and liability; we explore contractual aspects of trust and liability, since contracts form the basis of virtually all business-to-business interaction. Identity security must also meet legal parameters and establish a set of guidelines that result in defining an acceptable liability position for commercial and government usage.

Bridging identity security with the individual or machine needs to leverage existing application protocols such as the directory. The integration of directory and identity security is critical to linking individuals and to fulfill diverse and changing functions and roles. Typically, an individual is identified in a directory. A typical directory today contains some form of user credentials and, in some instances, application permissions. Many directories function as the "guard," the policy enforcement point in the enterprise. It is also can be a starting-point for most single sign-on environments.

The summation of an identity security model or IDSEC model can be defined in three fundamental security parts of Identity, Authentication, and Authorization.

Identity and authentication can be established with several technology elements. Before identifying identity elements, it is necessary to have their policy guidelines as defined in what constitutes authentication. The policy guidelines for determining authentication may be viewed as defined by the European Payment Authority and understood as the same in the broader security market.

The authentication elements for the purpose of strong customer authentication can be categorized as "knowledge," "possession," or "inherence":

- With regard to "knowledge" elements, these could be described as covering static passwords, codes or a personal identification number known only by the user.
- With regard to "possession" elements, these could be described as covering the possession of a physical object (a token) or potentially data controlled only by the Payment Service User (PSU).
- With regard to "inherence" elements, these could be clarified as covering biometric characteristics of the PSU such as a fingerprint or an iris scan." (European Payment Authority, Discussion Paper on Strong Customer Authentication and Secure Communications, 8 December 2015)

The model is illustrated in Figure 1 Identity, Authentication and Authorization.

Copyright 2016
All Rights Reserved

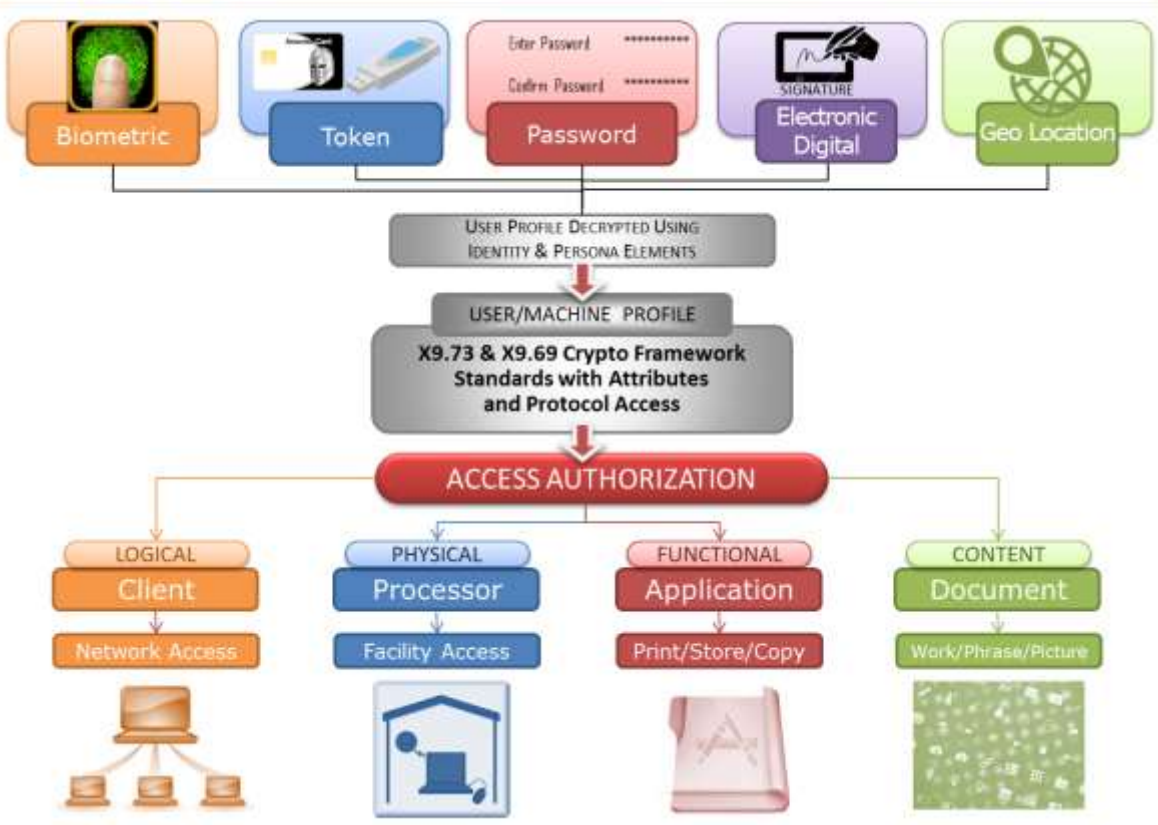

Figure 1 Identity, Authentication and Authorization

Identity Elements

There is no shortage of technologies that can be used for identifying people. Some of them can be used on their own; others have to be combined together to make them effective. A short list of the principal ones available today, together with some pros and cons, includes:

ID/Password/PIN

"A **password** is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

A **personal identification number** (**PIN**, pronounced "pin"; often redundantly **PIN number**) is a numeric password used to authenticate a user to a system, in particular in association with an ATM card.

The PIN is not printed or embedded on the card but is manually entered by the cardholder during automated teller machine (ATM) and point of sale (POS) transactions (such as those that comply with EMV), and in card not present transactions, such as over the Internet or for phone banking.

Copyright 2016
All Rights Reserved

> The term "PIN" is also now to refer to any short numeric password in other contexts such as door access, or unlocking of a smartphone screen." (Wikipedia January 2016, PIN)

An encryption schema may be integrated into a PIN authentication to add additional integrity to the process.

Log-on identification has been in existence for many years. An administrator issues people with individual identifiers (IDs) and an initial password. The user logs on and has to change the password to something new to ensure that it is a secret kept even from the administrator. Sometimes there are rules about how long the password is, letter or number combinations or special characters, how often it has to change, etc. It is cheap to implement and can be easy to administer. It can be used to enable cryptographic services. It is open to being stolen by many methods, and systems that do not detect too many attempts to use the wrong password are open to computerized attack.

Biometric

> "**Biometrics** refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.
>
> Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics to describe the latter class of biometrics.
>
> More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information." (Wikipedia Jan 2016, Biometrics)

There are many vendor applications which include one or more of the elements.

The financial sector has advocated a minimum of two identity elements to provide a statistical assurance of an individual or of an entity.

A variety of ways of identifying individuals by means of their physical characteristics are available. Each has its own requirements for registering people, and for implementation. If you intend to use one of these in support of the security requirements of your business process, you

Copyright 2016
All Rights Reserved

should check carefully that you are able to register individuals' biometrics suitably, and have a strategy for dealing with the situation in which the biometric reading device fails to read correctly an individual's selected biometric input even though it is the right individual.

Technologies here might also include:

- Voice
- Fingerprint
- Palm print
- Facial
- Eye retina scanning

The market is looking to take advantage of biometric functionality that have integrated sensing and no need for an external biometric reader. Voice, fingerprint, and facial recognition are two examples in which the computing platforms including mobile have sensing abilities to perform the necessary actions. Voice technologies have been in existence for some time. Master Card has announced in April 2016 that they plan to introduce in limited markets a pay-by-selfie and pay by fingerprint, as examples. The selfie technology would be based on facial biometrics.

Electronic Signature

"An **electronic signature**, or e-signature, is any electronic means that indicates either that a person adopts the contents of an electronic message, or more broadly that the person who claims to have written a message is the one who wrote it (and that the message received is the one that was sent by this person). By comparison, a signature is a stylized script associated with a person. In commerce and the law, a signature on a document is an indication that the person adopts the intentions recorded in the document. Both are comparable to a seal. In many instances, common with engineering companies for example, digital seals are also required for another layer of validation and security. Digital seals and signatures are equivalent to handwritten signatures and stamped seals.

Increasingly, digital signatures (associated with Public Key Infrastructure cryptography) are used in e-commerce and in regulatory filings as digital signatures are more secure than a simple generic electronic signature.[1][2] The concept itself is not new, with common law jurisdictions having recognized telegraph signatures as far back as the mid-19th century and faxed signatures since the 1980s.

In many countries, including the United States, the European Union, India, Brazil and Australia, electronic signatures (when recognized under the law of each jurisdiction) have the same legal consequences as the more traditional forms of executing of documents." (Wikipedia January 2016, Electronic Signature)

- An electronic signature, or e-signature, is any electronic means that indicates either that a person adopts the contents of an electronic message, or more broadly that the person who claims to have written a message is the one who wrote it (and that the message received

Copyright 2016
All Rights Reserved

is the one that was sent by this person). By comparison, a signature is a stylized script associated with a person. In commerce and the law, a signature on a document is an indication that the person adopts the intentions recorded in the document. Both are comparable to a seal. In many instances, common with engineering companies for example, digital seals are also required for another layer of validation and security. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. (Wikipedia 2016)

- Electronic signatures were earlier thought as public key encryption digital certificates, but legislature broaden the definition to include analog solutions. Different models for an electronic signature have surfaced in past years with no one method being predominant. A future direction can include an integrated encryption framework which would enforce the process and which could include a mix of analog and digital mechanisms.

GEO Location

"**Geolocation** is the identification of the real-world geographic location of an object, such as a radar source, mobile phone or Internet-connected computer terminal. Geolocation may refer to the practice of assessing the location, or to the actual assessed location. Geolocation is closely related to the use of positioning systems but may be distinguished from it by a greater emphasis on determining a meaningful location (e.g. a street address) rather than just a set of geographic coordinates." (Wikipedia January 2016, geolocation)

- GEO location is taking advantage of locator applications. A location is selected within a computing application, and that location action is further integrated into an authentication process to allow access or usage into a business application. For example, a laptop usage can be restricted to a specific geographic location. Encryption can also be included as an enforcement security tool.

Machine Identification

Machine identification is normally achieved in one of two ways:

1. *Manufacturer Identification* – this is where the manufacturer of the machine (computer, smart card, biometric device) provides it with a permanent and unique identification code. This may be a serial number or similar. The manufacturer uses quality control procedures to ensure there are no duplicates issued. Usually a special command to the machine causes it to reveal its identification code. This is the method suggested by the Trusted Computer Module consortium to protect the installation of software to a single machine.

Copyright 2016
All Rights Reserved

2. *User Identification* – this is where the controller of a machine provides it with a unique identifier. This may not be permanent or unalterable, although there may be operational procedures to prevent unauthorized change. The identity may be in the form of a serial number or it may be the installation of cryptographic keys. A special command can cause the machine to reveal its identity, or information being handled by the machine may be processed with a cryptographic key to prove it uniquely came from that machine (or perhaps that it was authorized by the owner of that machine).

Identities working with systems have different permissions and authorities associated with individual systems. These are exercised within management control processes maintaining an appropriate level of checks, balances, and accountability. These ensure that the identity performing the activity is appropriately authenticated and authorized, and that the level of monitoring of those actions ensures adequate accountability. The business control framework associated with identity, authentication, authorization, and accountability is termed "identity management." An audit and appraisal process ensures that the identity management framework is fit-for-purpose and operating as intended.

Vertical Market Identifiers

Business markets have used identifiers to accomplish identity security. These identifiers can take different usages. A more recent identifier within the financial services community is the Legal Entity Identifier which has been established as a fraud countermeasure.

e-Profile

One or more of the Identity Elements may be combined through an encryption method which results in an encrypted Profile file. To use the e-Profile, one or more Identity Elements are applied by an individual or by an entity for confirmation – an encryption key is activated by some process to decrypt an e-Profile file. The decrypted file contains sensitive data or sensitive information relating to its usage.

Figure 2 Identity Elements further illustrates a broader picture of the identities and their potential relationship to an e-Profile which includes crypto keys called Attributes that provide secure access to logical, physical, functional, or content applications. Various actions outlined in Figure 1 are contained in ANSI x9 standards, ISO standards, NIST standards, and protocol standards.

Token

"Token, an object which represents the right to perform some operation:

- Tokenization (data security), the process of substituting a sensitive data element
- Token, an object used in Petri net theory
- Session token, a unique identifier of an interaction session
- Security token or hardware token, authentication token or cryptographic token, a physical device for computer authentication

Copyright 2016
All Rights Reserved

- Access token, a system object representing the subject of access control operations" (Wikipedia January 2016, Token)

A token can be used as one of the factors in a multiple factor identity security solution, or a token can be a host device that includes security parts associated with identity, authentication, and authorization.

The token as one of the identity element factors for access control:

- A credit card-sized "calculator" type of device. After you have entered an ID/password, the computer system will send you a "challenge" which you have to input on the calculator and it will tell you the correct response that you then enter into the computer. It can be combined with ID/password in what is identified as "two factor authentications." A perpetrator would have to know the ID, the password, have the card, and type in the numbers correctly. The token may also need a password or Personal Identity Number (PIN) to get it to work.
- The token can be exampled as a smart card which can be used to store secrets, such as an individual's private encryption key for a public/private key process and/or the extended permission or authorizations that have been associated with that particular smartcard and to the person the card was issued. The security mechanisms on the card may insist that security operations (digital signing, for instance) can only take place on the card. It may require a PIN to be entered before it can be used, or each time it is used. This approach is particularly useful when mobility of the user is a requirement, or where remote dialog is the norm. The card can be an added trust platform to compliment other biometric elements.
- The token can be an integrated computing platform that includes one or more applications associated with various access control actions and includes encryption to enforce policies associated with these access actions. In lieu of a smart card format, the token can also take the form of a SIMM (Subscriber Identity Module) and an integrated reader to accomplish same access controls which could be done with the smart card.

Copyright 2016
All Rights Reserved

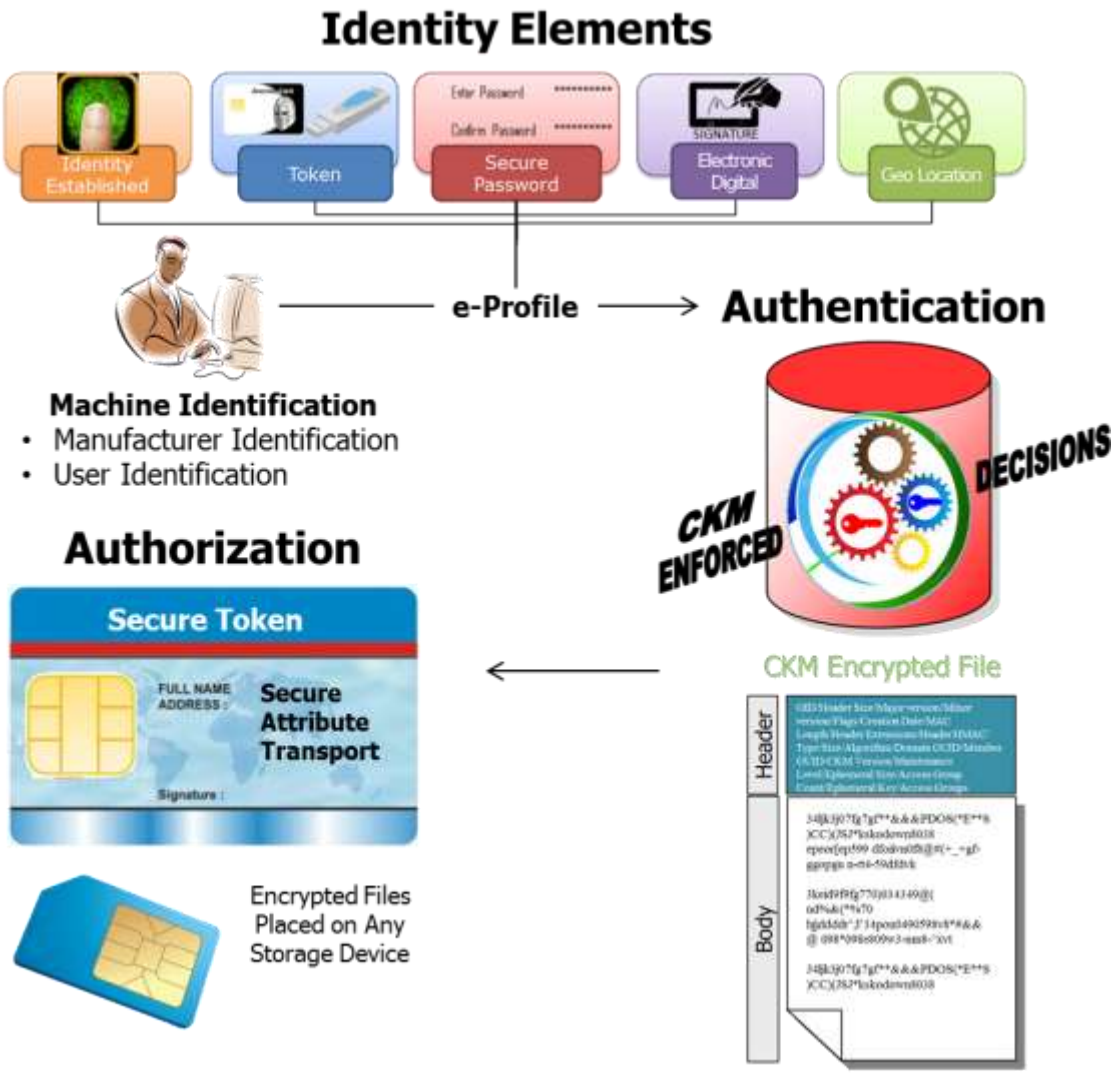

Figure 2 Identity Elements

Trust and Liability

The dictionary definition of trust is as follows:

> "Trust: firm belief in reliability, honesty, veracity, justice, good faith, in the intent of another party to conduct a deal, transaction, pledge, contract, etc. in accordance with agreed principles, rules, laws, expectations, undertakings, etc."

It is useful to remember some things that trust is **not**.

Trust is:

- Not transitive (cannot be passed from person to person)
- Not distributive (cannot be shared)
- Not associative (cannot be linked to another trust or added together)
- Not symmetric (I trust you does not equal you trust me)

Copyright 2016
All Rights Reserved

- Not self-declared (trust me – why?)

Management of risk and the issue of trust are governing progress in the whole field of e-commerce. The continuing development and growth of e-business depends on improving public confidence in using it, raising confidence levels to counter the whole range of security risks and vulnerabilities.

It is fundamental to a business that it will take risk decisions with every business transaction. As a consequence, a business decision-maker needs to be sure that the transaction will be completed to the satisfaction of both parties. Confidence that it will involves a process of gathering information to provide the decision-maker with sufficient information to enable them to make an informed risk decision.

To gather the information needed, the decision-maker often goes to third-party information providers to gather information – references, bona fides, credit checks, etc. – all aimed at building a confidence profile that the other party is plausible and capable of undertaking the deal involved. The use of third parties in business has been with us for centuries. The third party builds a reputation for delivering good or reliable information on trading companies, sometimes in a general business sense and other times in a niche.

Risk is, of course, based on assessing what the loss might be if something goes wrong, and whether you can absorb that loss if it does go wrong. Thus, we have levels of trust. For a small-value transaction, the degree of confidence in a trust assessment does not have to be large; for a multi-million dollar transaction, the level of trust needs to be very high. The required level of trust depends on your business policies on trust and risk management. A very common risk management approach is staged payments and bank bonds; another is to cover unacceptable financial risk by insurance.

Technology-dependent businesses need to enable appropriate risk decisions to be made. Trust services can be provided to automate steps in the business process to build trust, checking identity credentials on people and institutions, authenticating sources, etc.

There has been a tendency, by some, to misrepresent “trust” as a single process at a point in time, whereas trust is a process in itself. Trust is built or destroyed over time. Trust is generally subjective, though it may be supported by empirical information. This has resulted in the user community losing confidence in IT solutions providing a reliable basis for trust.

The analysis of a business transaction shows that multiple services are used in establishing trust. Some services are delivered by telephone, some by mail, and others by reference to a published source of data. There are also services delivered by lawyers, auditors, accountants, notaries, or other professional groups. Members of these groups are trusted to deliver correct information for various reasons, which may be important later in the digital delivery of these services.

Copyright 2016
All Rights Reserved

A person may decide as a matter of policy or individual case to delegate a trust decision to an automated process, another person, or a third party. However, responsibility for the decision rests with that person. Ultimately, the decisions on trust have to be human ones.

Given the general requirement to enable a business decision-maker to make an informed risk decision, it follows that during any business transaction the decision-maker will want to know what information they need to make the relevant business decision (risk decision). The information will come from a variety of sources. The decision-maker will trust (or not) the sources based on direct and indirect experience. Further, more trust means less perceived risk. More trust may be built by asking more questions of yet more information service providers. Alternatively, more trust may come from seeking information from a more reputable source.

Authentication

Authentication is the process of gaining confidence in a claimed identity. Once identities are issued, whenever they are used, there is the requirement that the person using the identity is the person that is qualified to use it. This is to minimize identity theft and is comparable to having to present another identity card whenever you use your credit card.

This requires a process for authentication and an authentication authority. Generally, the identity issuer tends to be the authentication authority. When the only requirement of the identity is uniqueness from other identities, the process of authentication may be quite lax. As the requirements become more stringent, the process evolves from a simple password to two-factor validation and beyond.

Authorization

Authorization is a process of granting or changing rights (permissions) and carries with it the scope of authority, which includes the granting of access based on agreed access rights (see ISO/IEC 7498-2). It is a security control that defines and provides the means of granting access after verifying the authenticity of an individual's identity and level of authorization to receive specific categories of information or to carry out defined tasks.

Authorization is directly linked to authentication. Generally, once an entity has been successfully authenticated, the directory provides credentials to IT business services and applications supported by the infrastructure. Consistent and clear levels of authorization can simplify and reduce complexity and costs. Among the levels of authorization, standards can be a baseline set of permissions to access, read, and modify data.

Revocation

Revocation is the process of rescinding an identity or permission that has been granted. This is a process that must be properly recorded for audit purposes. This is required to prevent continued use of the identity under potentially false and insecure contexts. If not done properly, this would open the identity authentication authority to potentially significant liabilities.

Copyright 2016
All Rights Reserved

Starting with the idea that trust gets translated into the notion of authority, it follows naturally that authorities become the agents of provisioning.

- Account provisioning, which deals with identity-related information associated with individuals, their personal attributes, affiliations, etc.
- Resource provisioning, which deals with business assets such as computers, databases, and applications and the management of permissions associated with those assets
- Account de-provisioning, which deals with the termination of access rights to systems and services and re-allocation of those systems and services.

Multiple authoritative sources may exist in an organization (HR feeds, systems providing financial data services, directories, etc.). From a best practices and manageability perspective, it is important for an organization to make one authoritative source the main source of identity information (e.g., hiring information, identity's credentials such as user name, social security information, salary). This will help prevent information being fraudulently entered when provisioning an identity into an organization. Receiving, validating, and pushing up-to-date information to the appropriate feeds is important to consistently manage identity information.

As identity management grows and matures, and especially as its use outside of the organization grows, the publication aspects of the directory services underlying the identity management facility will become especially important. This is for two basic reasons:

1. The directory will have to publish information.
2. The directory will have to protect information.

As a publication vehicle, directory technology today is mature and ubiquitous. The Lightweight Directory Access Protocol (LDAP or MS Active Directory) is ideally suited to access information stored in directories – be they LDAP or X.500. It is a well-understood protocol and there are many tools available to developers for creating applications that will utilize directory information.

Directories, typically, have not been the "decision-maker" in authentication, authorization, or policy interpretation. They have contained the requisite data, but other applications have taken that data and rendered an appropriate decision. There are exceptions, of course. For instance, Network Operating System (NOS) Directories, such as Active Directory and e-directory, do make numerous identity management authentication and authorization decisions based on the ability to match credentials supplied by a user or system with the values (securely) maintained in the directory.

Without standards-based access controls and a standards-based policy interpretation mechanism, the "making decisions" capabilities required of identity security will continue to be performed, predominantly, by the application and not by the directory. Separate access controls utilize the results obtained from the directory to provide whatever permissions are available to the authenticated submitter.

Copyright 2016
All Rights Reserved

Most general-purpose directories today do not function as "enforcers", but as traditional repositories – leaving the enforcement to the target application. Concepts such as "Groups", "Roles", etc. could then be much more efficiently utilized. The enforcement component can be an encryption framework and that framework would leverage financial frameworks found in ANSI, ISO, and NIST standards.

Access Control

Access control refers to the control mechanisms that ensure access and permissions are given to all those who have the required access rights (an authenticated user with the required bindings) to perform specific operations on the resources within that system. This same mechanism denies access to unauthenticated users and to authenticate users if they attempt to perform any operation that they are not authorized to perform.

Systems relying upon access controls usually have lists of the users who are allowed to access the various resources available within it, together with the rights that they have. These rights can be exerted within or by different parts of the network. Access control can begin at the login process and the network can control various accesses to applications and server locations or connections that reside within the network control. The relative owner of the information can exert further controls as it is moved throughout the enterprise. This separation of control is very useful as the Network is only capable of managing access at a relatively high level, and today's information controls have fine grained access requirements to the object level (a field within a record for example).

Access control can also be extended to identity, authentication, and authorization.

We are familiar with what identity and authentication mean. Authentication checks the computerized identifier back to the specific person or specific computing component to which it was originally linked. Authentication can also be used to bind the authenticated user to what that user is authorized to do, the result being a profile of permissions allowing that user to perform specific operations on resources in the computer system, for example:

- To access data files, with permission to do any one or more of read, write, append, and delete
- To access programs, commands, utilities, etc., to execute them, modify them, etc.
- In networked systems, to access other computers and the resources within them
- To submit forms and to electronically sign those forms

Further, the authorization component can be used as a mechanism of control to limit the specific users' access to information within a form.

IT business policy provides two sets of information in the system:

- IT defines the authentication and binding rules for users
- IT defines the operations allowed on computer resources

Copyright 2016
All Rights Reserved

Authorization in business terms refers to a person or an operational entity having gained the required authority or permissions to do an operation or task.

In computer systems, authorization is where the system administrator or similar authority translates a user's (or a specific group or class of users) permissions to access a designated set of system resources – data files, programs, specific functions and commands, networked facilities, etc. – into computer-recognized form for binding to that user's authenticated identity.

In a PK (Public Key) environment, authorization information may also be provided to an established identity. This function is managed by the introduction of a complimentary mechanism rather than using the PK certificate alone.

These principles come from the world of audit controls, where in order to reduce the risk of fraud; no user should be in a position where they can act without anyone else being aware of what they are doing. Unfortunately, many IT systems were not designed with this approach embedded in their control structures, and as a result, many existing computer systems have "super-users" who have what is sometimes called "root" powers that give them unconstrained authorization to do whatever they choose.

Such capabilities, without authorization controls, create ideal conditions for hackers. There is also the requirement in some organizations to constrain access to information on a "need to know" basis. Although traditionally a military term, "need to know" can also refer to the individuals "justification or rational"; as in the case of patient identifiable data.

Identity Security Controls

Identity security in many organizations starts with an appropriate risk assessment to determine the need for identity management controls to properly protect information, applications, and infrastructure as required. These controls set the lifecycle security objectives for creating and maintaining an identity, verifying and authenticating an identity, granting permissions and authorities, monitoring and accountability, and auditing and appraisal of the identity management processes.

The fundamentals of identity security define the control objectives for:

- Identification - the security control process that creates an entity and verifies the credentials of the individual, which together form a unique identity for authentication and authorization purposes
- Authentication - a security control process that verifies credentials to support an interaction, transaction, message, or transmission
- Authorization - a security control process that grants permissions by verifying the authenticity of an individual's identity and permissions to access specific categories of information or to carry out defined tasks

Copyright 2016
All Rights Reserved

- Accountability - a security control process that records the linkage between an action and the identity of the individual or role who has invoked the action, thus providing an evidence trail for audit or non-repudiation purposes
- Audit - a security control process that examines data records, actions taken, changes made, and identities/roles invoking actions which together provide a reconstruction of events for evidential purposes

All the control objectives above serve the requirement to provide an auditable *chain of evidence* using a *chain of trust*. The chain consists of linking and binding the fundamental security controls that define the control objectives. Encryption can be the binding mechanism like a secure envelope which contains these fundamental controls as applications.

Control objectives apply to individuals and roles and their actions on the enterprise infrastructure. The result is the establishment of a baseline identity security reference for identities created, recorded, and managed throughout their lifecycles in applicable directories. Standards codify the mechanisms associated with the fundamental control.

Many organizations have both vertical and horizontal business structures. These structures are continually forming, merging, acting, splitting, and dissolving. Identity management must play its complementary part in these processes.

A complete identity security architecture has more components than just security. The framework of an identity management solution has several key components:

- Enterprise information architecture
- Permission and policy management
- Enterprise directory services
- User authentication
- User provisioning
- Workflow
- To enable an individual to verify and authenticate a claimed identity
- To establish consistent standards of authentication in the infrastructure
- To establish a baseline for verifying and authenticating an identity

Authentication is a process to verify claimed identity (see data origin authentication and peer entity authentication in ISO/IEC 10181-2). This is also defined as a security control that establishes the validity of an originator's credentials, message, or transmission.

Persistent Protection of Data

A final area of concern for identity security is the provision of persistent, data-focused protective measures. By this, it is meant that it is necessary to provide the ability to protect data independent of its deployment on any particular platform or its use by a particular application. As the use of XML becomes increasingly prevalent, the existence of data apart from platforms and applications will become increasingly common, and it will be necessary to provide

Copyright 2016
All Rights Reserved

protection in the form of integrity, confidentiality, and privacy, and in the process, preserve certain pieces of data as forensic evidence.

The use of permissions are also fundamental to the control of, or access to, information, to services, and electronic forms.

Mechanisms exist for providing the basic capabilities associated with these services, using a combination of symmetric and asymmetric encryption, time-stamping services, message digests, and digital signatures. What is missing is the association of any of these mechanisms with a common core identity. It is believed that the use of the common core identity mechanism in conjunction with the existing cryptographic and time-stamping mechanisms will be sufficient to provide the desired protections necessary to securely engage in electronic business communications.

Over the past few years, there has been much effort to establish a mechanism for the establishment of identity on a large scale. Commercial firms have been engaged to register information about individuals and manage that information as a "neutral" arbiter. On the surface, this seems like a reasonable function and business opportunity. The industry as a whole also recognized that there needed to be some overt declaration that explained and defined just what would be involved in this service. This declaration is called a Certificate of Practice Statement (CPS). However, when examined, the most a CPS can really offer is that a procedure of registration was followed. There is no possible way that any third party can vouch for a person's identity without also offering some level of assurance or liability to the action of establishing that identity. This idea of liability has, to this date, never been satisfactorily addressed. Even the most stringent examination of the reference material submitted (commonly called "seed" material) puts the examiner in the awkward position of having to be an expert on determining identity. This is made even more difficult when one considers the record keeping of different municipalities in these United States over the past 100 years. Birth certificates are available, from some States (Pennsylvania for example) over the Internet. Other States offer photo copies of a handwritten document with no official seal or validation other than the written signature of some otherwise unidentified hospital employee, or in some cases, a simple telephone conversation may be the only assurance available. Driver's licenses are routinely made available for a fee, and very little else. There are sources on the internet that will provide a driver's license for any state in the US, with any identity, combined with a very nice photo, that are accurate enough to pass as genuine to all but the most detailed, expert, examination.

What this means is that, in the final analysis, the parties must, at some point establish trust directly. Without the associated liability, trust is not transferable.

Options for an Identity Security

There are options for a solution to consider:

Copyright 2016
All Rights Reserved

The first step is to define the objectives or requirements that must be met. The need to take advantage of the efficiencies of the Internet is clear. Time is money, and the nearly instant communications vehicle of the Internet offers not only savings in time but also in the immediacy of the response given to a request, service, or business transaction.

Registration over the Internet could be a desirable component of the solution.

Step two is to establish a trust mechanism that will allow the organizational owner of the relationship (as opposed to the members' role within the organization) to manage the relationship in a trust assuring manner that is both cost efficient and serviceable over time.

The issuance of an identity token would be one component to consider. The issue, after all, is one of identity, and an identity, at its base, is unique. Software can be copied, corrupted, or otherwise altered and does not lend to a high degree of assurance. Of course, there are costs tradeoffs that will impact what would be an acceptable risk.

The token, as the focal point of control, would need to store, and ideally apply multiple factor identity elements for access control. Further, the token should be able to act as a "federation" device, storing the various authentication and authorization applications that would be extended by the different departments or even by multiple enterprises, to that unique token and the unique individual to whom it was issued.

The token should be able to be serviced, or updated, remotely. Over time relationships change, roles are modified, privileges are extended and withdrawn, and all of these alterations need to be accomplished, in a secure manner, across the Internet.

The central issuance of the Identity Token by a given enterprise is a matter of efficiency and also logical coordination.

In addition to the digital components for a solution, other security methods need to be considered such as handling the token in an approved secure channel. The use of the card and its security framework can be executed under a Certificate of Agreement.

Once in the hands of the appropriate user, the issued token offers a unique identity security platform which can be exercised by the insurer as well as by any other organization the issuer might authorize.

This is one possible model that could take advantage of a combination of existing technologies and laws to arrive at a cost effective managed level of trust, and still be deployable over a large population.

Copyright 2016
All Rights Reserved

Section 2 Distributive Ledger and Blockchain in Security Preface

The Distributive Ledger is emerging as a new tool for doing business. A recent Guardian commentary summed up their view with the following: *A distributed ledger is a special kind of database that is spread across multiple sites, countries or institutions, and is typically public in the sense that anyone can view it. Entries in the database are configured in "blocks" which are then chained together using digital, cryptographic signatures – hence the term blockchain, which is really just a techie name for a distributed ledger that can be shared and corroborated by anyone who has the appropriate permissions.* (The Guardian, John Naughton, 24 January 2016). The United States financial sector is developing their concepts in parallel with other international bodies.

This paper is identifying a concept that includes a Distributive Ledger and the supporting Blockchain technology based on standards, on public digital technology, on private digital technology, and on IP technology.

Blockchain can exist for various segments identified with security. As an attached document, **Annex A** broadens the scope of security to include security categories that can define the enterprise security environment. Information security is one of the security categories and is the focus of this document.

Introduction

The financial community is looking for a faster and more secure payment system. Many events have given inertia towards a new way to do banking from the traditional methods. Much has been written, and it is anticipated much will be written, regarding digital payment methods.

The current digital discussion has also expanded into the subject of alternative currencies such as digital currencies. In recent time, a model has emerged which had genesis with a digital asset platform identified as Bitcoin. Basically, the Bitcoin architecture includes three fundamental parts:

1. A Miner or the entity which would generate something digital that could be used as a means of exchange,
2. A means of communicating the exchange, such as the Internet, and
3. A settlement process between two persons who would have something to sell and a purchaser who had the Miners digital value representation.

Bitcoin was able to demonstrate that a faster financial exchange was possible which included a Hash math function for their security. Since Bitcoin's emergence, many business models have emerged including Blockchain and Distributive Ledgers. In some instances, variations with Bitcoin are in the financial market. But, the financial community has also put forth alternatives to Bitcoin with a goal of a secure, faster payment.

Copyright 2016
All Rights Reserved

The encryption found in the Blockchain cryptography, and the ledger concept identified with the financial services, may have applicability in other vertical business markets beyond the financial sector.

Building a secure Blockchain Distributive Ledger includes cryptography of the Blockchain and a defined group of *Blocks* or equivalent *Transaction Components* that constitute a financial services transaction model.

Blockchain can be defined as an encryption framework which ties financial services components as blocks with secure linking among the blocks or components while enforcing access to each of the components. Blockchain can also be expressed as a group of blocks that are linked, or chained together, in a way that the information stored in each block is secure and time-stamped. The resultant secure blocks may be distributed across a network and accessed in a Cloud.

Within the financial sector, Blockchain security technology offers an innovative method to implement financial ledgers, the records of buying and selling stocks and bonds, or just about any type of transaction. For example, a bank can track the deposits of all their customers in a ledger maintained by the bank while including other financial services such as audit and settlement that would be associated with a transaction.

As an alternative digital architecture, a ledger operation can be modeled into a distributed ledger using Blockchain technology and establish which financial components can be absorbed outside of a bank role. Using a distributed ledger in this manner can reduce cost and have a faster payment result. However, trust, liability, and acceptance within the financial sector must be included with the Blockchain-ledger model.

A Blockchain model with accompanying financial components is illustrated in Figure 3.

Copyright 2016
All Rights Reserved

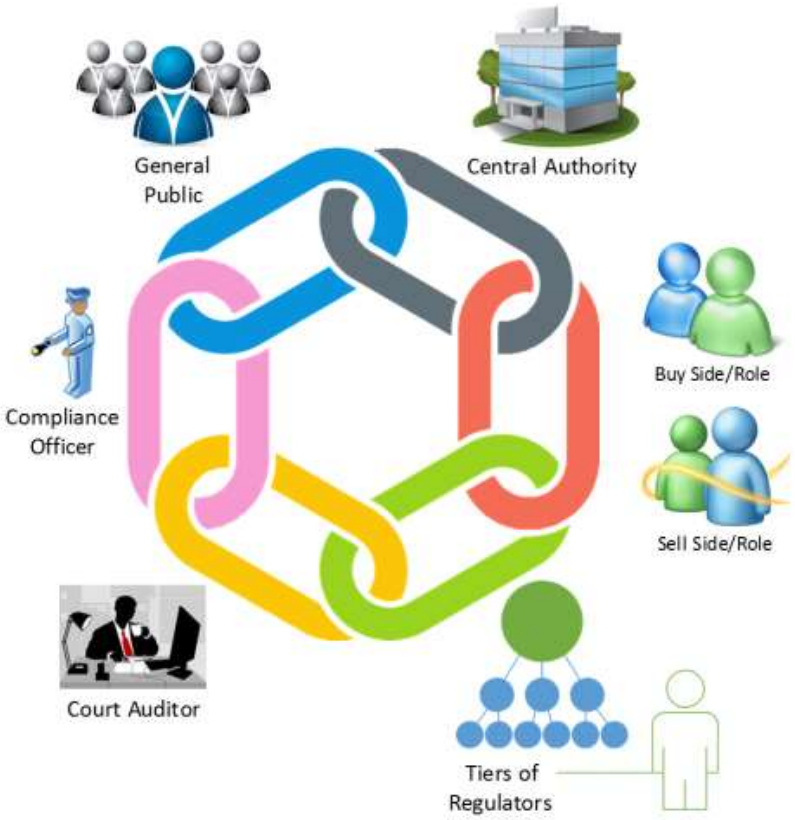

Figure 3 Blockchain Model

Identified are seven Financial Services Components representing blocks that can be associated with a transaction. Major components include: Buy, Sell, Regulator, Audit/court, Compliance, Public, and Central Authority. Each component has actions which are part of a ledger process and ensure the integrity of a transaction.

Blockchain as a Secure Envelope with Identity and Encryption Enforcement

Securing Blocks of Financial Data

Inherent in a discussion about Blockchain is a capability to secure blocks of data which can be attributed to a financial transaction. Each block can be illustrated as a unique envelope, and each unique envelope, as well as the overall envelope, can be linked with a Blockchain encryption. Figure 4 Secure Transport Envelope illustrates this concept.

A S*ecure Transaction Envelope* schema includes *identity and encryption* for secure access control as pictured in Figure 4. The intent is to front end each financial services component (or 'Object') to provide authentication and authorization. For this illustration, a Purchase Order is one of the financial components. An outer envelope identified as a *Transport Envelope* defines a collection of financial components in which each component itself may have their own identity and encryption schema.

Copyright 2016
All Rights Reserved

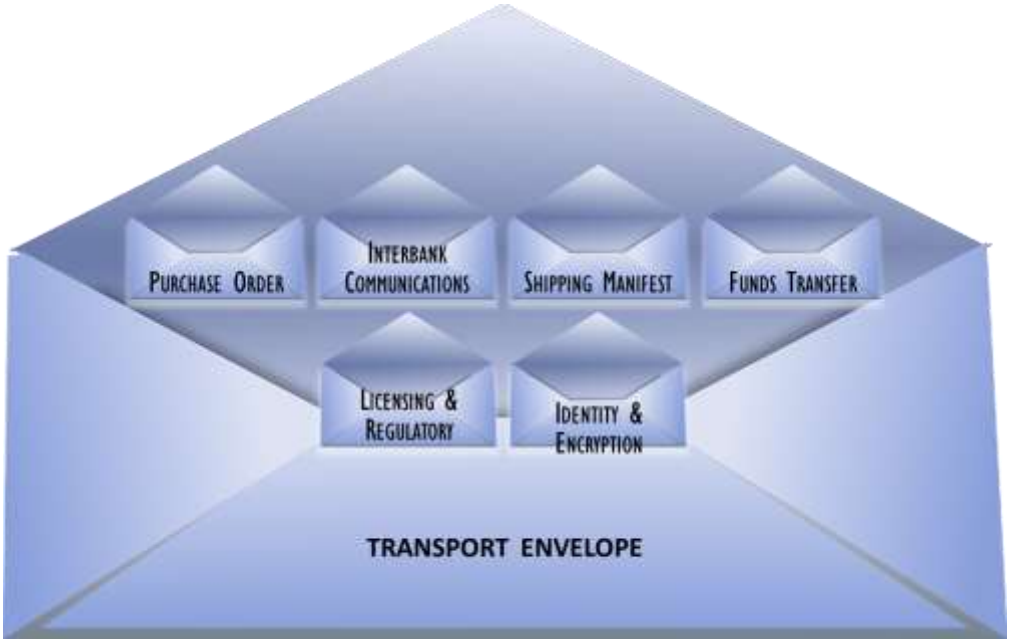

Figure 4 Secure Transport Envelope

The following Transaction envelope contains a business application for a Purchase Order. Figure 5 illustrates six financial components that are identified within a financial transaction. This illustration and discussion will presume that all the components are identified with current legacy financial transaction architecture and supported by a banking authority. The banking authority may be established in a different transaction authority outside of traditional bank.

Figure 5 Purchase Order Transaction Envelope

Imagine that the envelopes in the previous figures were each sealed, much as sealed envelopes are circulated through our postal system. The sealed envelopes could then be considered a

Copyright 2016
All Rights Reserved

linkage to the past when mail was a financial instrument. A sealed envelope had identity and access control defined by the Postal regulations.

A digital secure envelope can consist of N*ested Secure Envelopes* which provide further granularity to specific component actions. A sample use case can consist of a secure envelope which manages access to the various Ledger components, or a use case can be extended into a focus on one or more components within their operations while leaving other components left to an access level so that proprietary or legacy applications can be applied. The legacy-encrypted envelope for a first level access may be viewed as a nested secure module in which the front end access function is encrypted in a self-contained encrypted module and that encrypted module is applied within the main Blockchain linkage.

Now we have a digital world that is looking to link the security of the past into security for the digital future. To relate to the digital world, an understanding of Objects is important.

As an attached document, *Annex B* provides a discussion on Defining Objects for a Digital Currency in which the analog envelope can be defined with its objects. In the attachment, the concept of objects is further linked to objects in a payment schema, and finally suggesting that objects can be the starting point for identifying what security elements can be available.

Copyright 2016
All Rights Reserved

Blockchain as a Crypto Process for Differential Access

Figure 6 is an illustration of a financial report for which differential access is applied through a cryptographic framework.

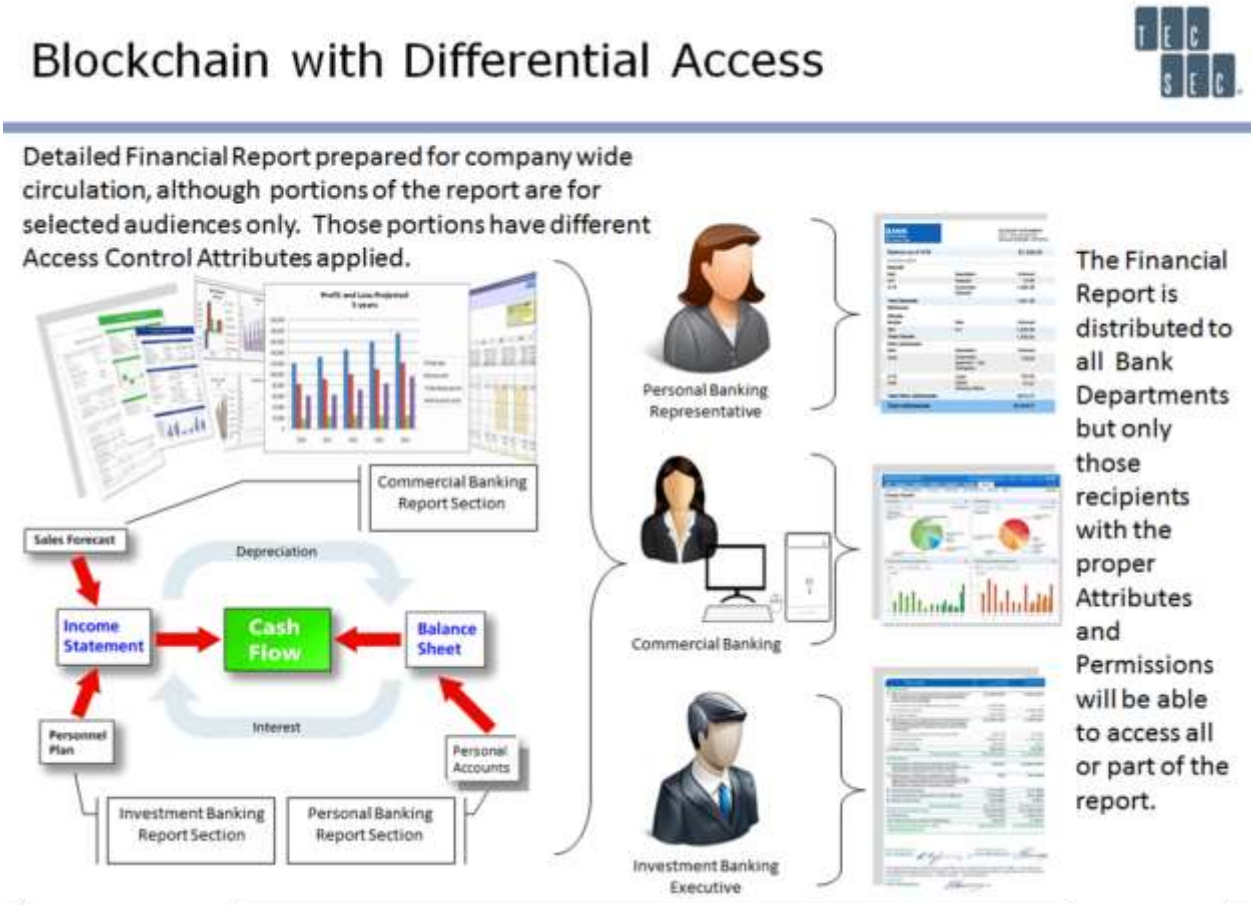

Figure 6 Differential Access on a Finance Report

The intent is to provide access to parts of the report that are needed among the various banking departments. An analogy would be a carbonless form in which sections of the form would be accessed by only authorized individuals. Looking at Figure 7, entries for bank and descriptions may be only accessed by a compliance officer while the voucher's other parts could be processed by others. The makeup of the voucher form would offer or require different levels of authorization.

Copyright 2016
All Rights Reserved

No. 0001

PAYMENT VOUCHER

Company Logo

Date: _____

Paid To.: _____

Paid By	Cheque Details		Date	Description	Amount
	Cheque No.	Bank			
Cash ☐					
Cheque ☐					
Total					

Amount in words (AED): _____

Prepared By: _____ Approved By: _____ Received By: _____

Tel : +971 4 123 1234, Fax : +971 4 123 1234, P.O. Box : 126534, Dubai - U.A.E.
www.yourcompany.com

Figure 7 Payment Voucher

A Blockchain Encryption Framework

Encryption is an essential part of a Blockchain architecture. From a technical perspective, the Blockchain encryption must ensure the integrity among blocks of financial components, it must encrypt the links among the blocks, and it must provide persistent enforcement for the block's content. From a functional perspective, the *Blockchain encryption framework* must address the following necessary actions:

- Handle scale,
- Be able to model different encryption parameters which the financial sector defines,
- Be able to integrate into the digital Internet and banking legacy architectures, and
- Be able to enforce privacy and liability.

A standards' based encryption schema exists as defined in ANSI x9.73, Cryptographic Message Syntax standards, and supported through other standards. X9.73, Annex D, details an encryption framework that results in a dynamic encryption process with a changing key for every encryption action.

Figure 8 is an illustration of the elements associated with the x9.73, Annex D, encryption framework identified as Constructive Key Management (CKM®).

Copyright 2016
All Rights Reserved

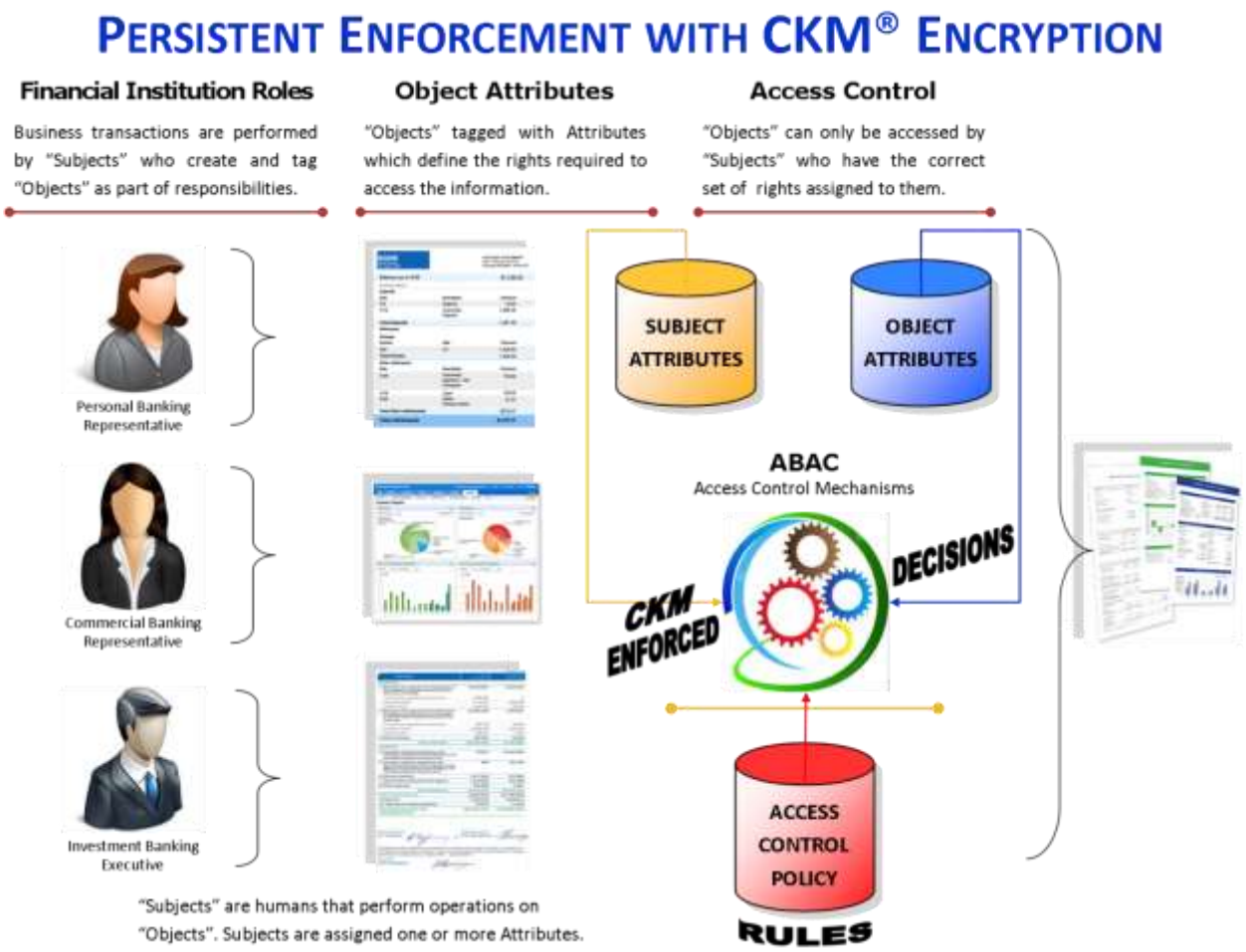

Figure 8 Persistent Enforcement with CKM Encryption

CKM encryption relates information to a mathematical encryption schema. The Figure 8 illustration identifies key steps in the encryption process. Roles as subjects or objects are assigned responsibilities that need access enforcing. The examples in the illustration above are different representatives and personnel, but roles also can be attributed to actions within a financial institution such as a transaction's financial component access. Tied to these roles are attributes which act as the bridging agent between information and the crypto framework. The attributes define the rights required to access information associated with the roles. The execution of object access, as it relates to roles, can be further characterized in the illustration's final access control section. Note that rules for access control can be applied with the marriage of parts within the access control mechanism. The encryption becomes an enforcement agent for the rules.

The CKM process is unique, but contains standard based algorithms which are combined to create a unique secret key. The CKM combiner can be tailored to the security level desired to protect the data. A CKM framework can provide confidentiality associate with cryptography and its secret key. Blockchain encryption needs confidentiality and the high assurance of the math association with cryptography. As a Blockchain is applied to a financial ledger, the resultant

Copyright 2016
All Rights Reserved

transaction and security are important to the institution that needs to measure liability and privacy. Cryptography has demonstrated an ability to be another tool for the business manager to gauge risks.

The data associated with the transaction components is included in an E*ncryption Envelope* to ensure security integrity of a component and a security linkage within the transaction process. A naming convention is found in *attributes* which form a set of permissions, and these same attributes include math which is bound to the CKM encryption schema. The Central Authority component may be a bank or other financial services entity and is responsible for managing the encryption. The CKM encryption framework includes a standards based random number that changes with each cryptographic event to ensure integrity for the encryption process.

Permissions as Enforcement Attributes

The CKM framework includes attributes which define access to the encryption envelopes associated with the transaction component actions. The permissions allow different levels of access. Figure 9 includes a sample representation of financial component actions associated with permission attributes.

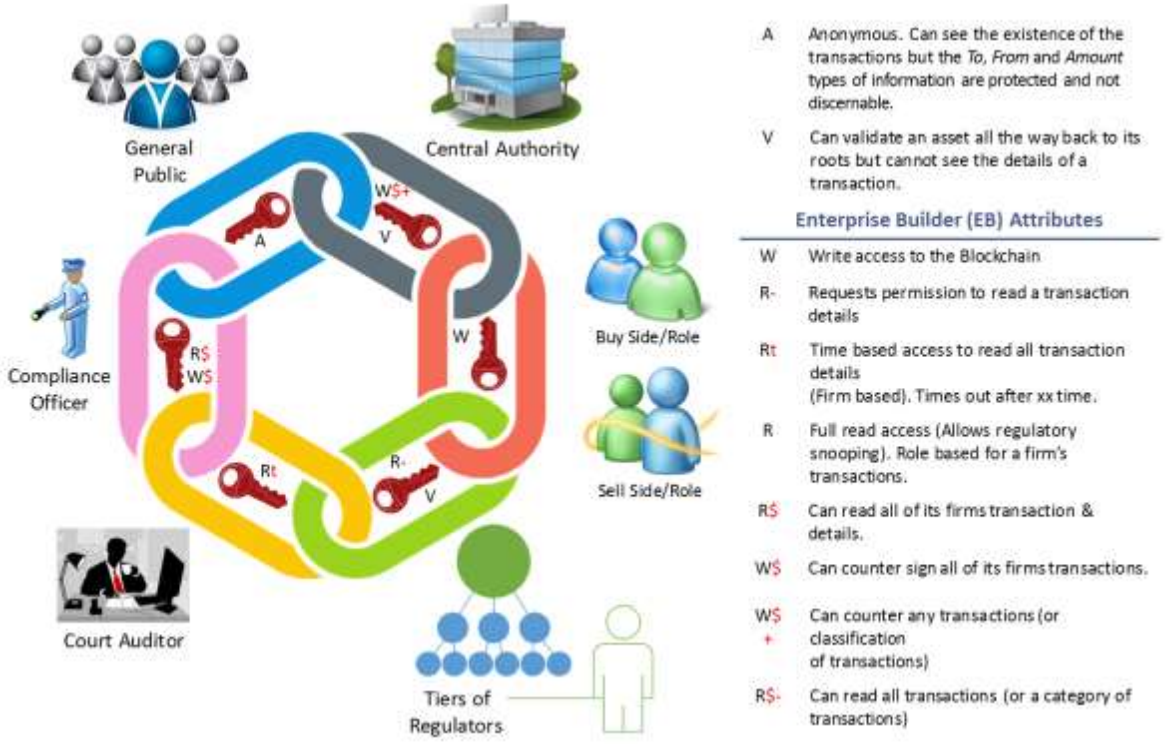

Figure 9 Financial Service Components in the Blockchain

Copyright 2016
All Rights Reserved

Attribute Listing for Financial Services Components

The following is a sample attribute listing for the major financial services components. Additional attributes are possible to add to the list based on the extent of granularity and on the extent of connectivity within each component's specific application or module.

Table 1 Financial Service Components

Component	Attribute	Usage
Central Authority (EB)	*PlainTrans*	Anonymous. No details of To, From, and Amount
Central Authority (EB)	*BankAuth*	Share transaction data with other financial institutions. Read or Write encryption authority exists
Buyer (Purchaser)	*Buyer*	An entity who or which has funds to buy goods
Seller (Supplier)	*Suppler*	An entity that has goods to sell
Regulator	*Regulator*	May be limited to Read only or, Buyer's Read Only for a specific transaction part.
Court Auditors	*Court*	Access level determined by Central Authority (Each financial institution has established their policy to work with compliance) Read, Write, or Full access options.
Compliance	*Compliance*	Access level determined by Central Authority (each financial institutions has established their policy to work with compliance) – Read, Write, or Full access options.
High Net Worth Entity	HighNet	To identify a high net worth person or entity
Application Access Control	AppAccess	Front end linkage to financial services components using encryption

Background Material Associated with Financial Services Components and Attributes

The following alpha indicators are seen in the blockchain transaction shown in Figure 9:

- "A" says that the existence of a transaction is visible to anyone but the To, From and Amount types of information are protected and not discernable. There may be instances where the amount is not protected. Central Authority has an enterprise key manager that controls the creation and distribution of all attributes related to the creation and validation of the chain.
- "W" and "V" are actually the read/write components of an attribute for the Blockchain itself.
- The other R's and W's are from an enterprise key manager that is controlled by the firm, group or person to which an account in the Blockchain is assigned.
- A record in the chain has a portion encrypted using "W". The transaction details (From and To) are separately encrypted using the firm's Attributes in any mix as appropriate for that type of transaction (determined by the firm). This provides a form of protected identity, anonymous to the outside world but visible for internal tracking, auditing and regulatory issues.

Copyright 2016
All Rights Reserved

- Shares can be issued from either or both of the Central Authority and a Firm's enterprise key manager to allow for the read of the required level of details by courts/auditors/regulators.
- The encryptions can be bound together cryptographically.

Table 2 Financial Service Component and Access Permissions

Component Person/Role	Description/means of access through Attribute Permissions
Central Authority	The Central Authority holds an EB that controls the creation and distribution of all attributes related to the creation and validation of the chain. Manages the overall Blockchain and has the "V" and "W" components. The Central Authority issues the "W" component to each player that has the ability to create transactions. Note there may be multiple "V" and "W" components for different types of customers/transaction sizes.
Buyer/Seller	Has firm based attributes so that they can create/read the details of a transaction. This can become a web of relationships between a buyer and the sellers from whom they purchase items. The buyer initiates the transaction as they are transferring money from their account to the appropriate seller. The seller may or may not have the ability to read the buyer's details. The transaction itself would have a unique identifier that the seller could internally link to their own records. If the buyer works with a seller a lot, then they COULD grant the seller the "R" portion of the attributes for the Transaction Detail records from that buyer to that seller. The buyer could use any combination of internal attributes also for the firm's internal book-keeping and processes.
Regulators	Regulators can have a variety of needs. Sometimes they would just need to validate the integrity of the transactions. In that case, the Central Authority would grant them the "V" component for the transactions in question. Other times they need more transaction details. In this case, the Firm's (buyers) would either grant read access to the transactions or issue "Shares" for the particular transactions in question.
Court Auditors	This role is very similar to the Regulators. It is more likely however that both the Central Authority and the Firm would issue "Shares" for the exact transactions in question.
Compliance Officer	This person would be issued the read attributes from the Firm and also potentially, the write attributes.
General Public	The general public would not be issued any attributes from either the firm or the Central Authority. They could only see that the transaction exists and the public information in the transaction.

A Secure Packet Based on a CKM Header and Linkage to Transaction Details

An overall high level view of a Blockchain packet flow could look like the Figure 10 illustration:

Copyright 2016
All Rights Reserved

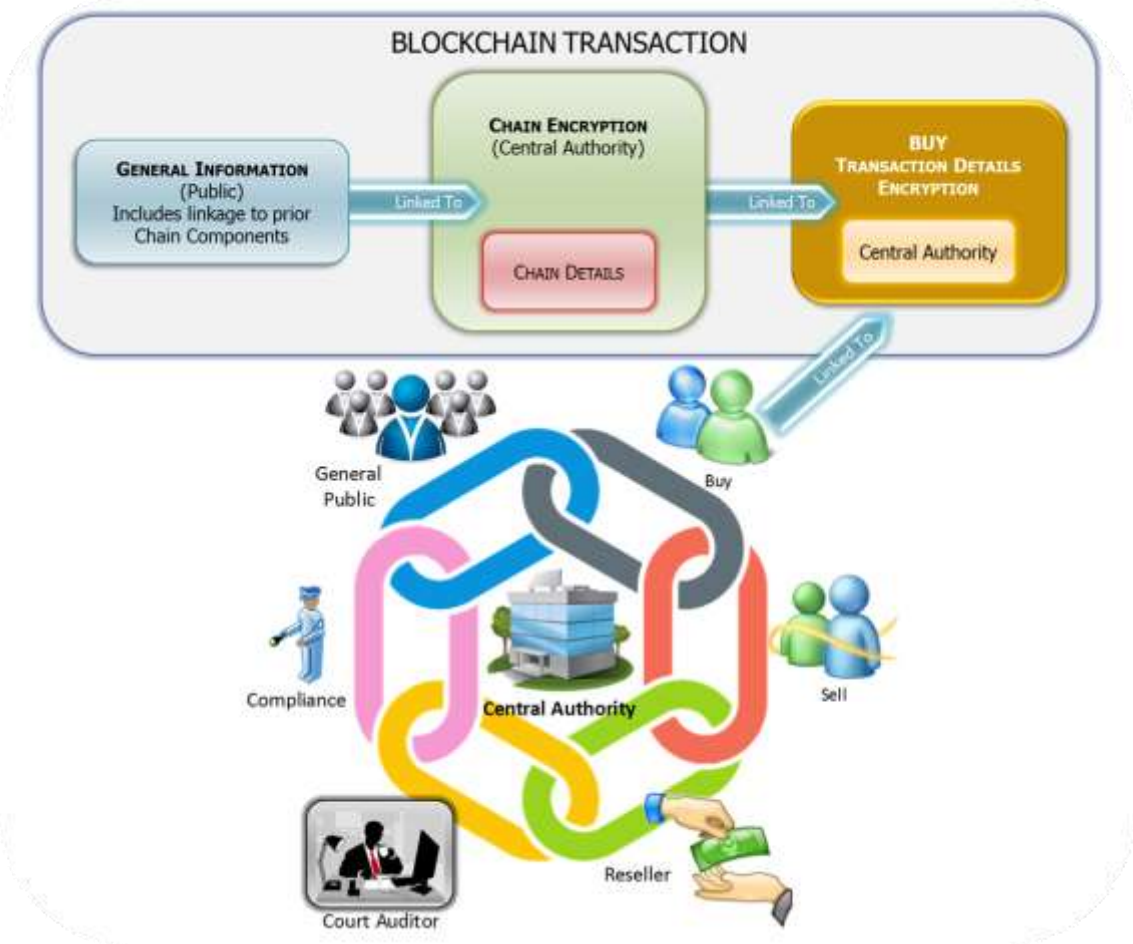

Figure 10 Blockchain Packet Flow

The Blockchain illustrated in the previous Figure 9 is presented as a set of financial component blocks which are chained together with to-and-from links bound by the crypto attributes of the Central Authority. One of the components, the BUY component, is further detailed in Figure 10. The basic architecture would be applied to other components to complete the linkage among the financial components.

Within each component can be further content protection using the same architecture, but the protocols may differ to embed the Blockchain mechanics.

Copyright 2016
All Rights Reserved

Section Three Blockchain Usages Introduction

To explore usages for Blockchain and accompanying ledgers, there are issues and directions which need be included as decision factors.

1. Blockchain encryption can eventually become a means to alter existing financial services infrastructure, but not by itself. Blockchain needs to take into account the Internet, Identity & Data Protection, and Legal guidelines.
2. From an alternate view, access to the data must include authentication and authorization security techniques.
3. Employing Objects to define the data:
   - Objects to facilitate processes associated with manipulating the data,
   - Objects can be the basis to define the Blockchain encryption engine,
   - Objects to establish an encryption framework which binds encryption to the data directly, and
   - Objects which include a framework mechanism for attribute permissions to manage access to the data.
4. Secure objects allow the access controls for its content to be integrated with the object, regardless of where the object is stored, the data is secured.
5. The Blockchain encryption framework needs to accommodate a mix of cryptographic encryption algorithms to accommodate international usage.
6. Each object encryption action results in a new encryption key. A compromise of that one key limits access to that one key's data. Subsequent data encryptions use new and unique encryption keys.
7. Existing standards have the integral security elements needed for a Blockchain encryption and Distributive Ledger architecture.
8. An exemplar object oriented encryption framework is defined in ANSI x9.73 and ANSI x9.69 as a dynamic encryption syntax identified as Constructive Key Management.
9. The ledger may be public or proprietary. A proprietary ledger includes Identity as an essential differentiator. The intent of the Public ledger is to allow financial inclusion without access to existing financial services (unbanked, underbanked, and unbankable).
10. With cryptography, National and International export controls must be considered.
11. The Blockchain-Ledger schema must be able to accommodate new advances in cryptography, in communications, and in Internet protocols.
12. Identity and authentication may be considered as fixed to an individual or to an entity; whereas authorizations are changing to definitive access requirements relating to financial services.

Copyright 2016
All Rights Reserved

13. Secure yet configurable access is need to varying levels of sensitive data.
14. The fixed Identity design must be able to be movable to accommodate the potential different data access authorizations.
15. Codified business processes can't be skipped because of the mathematical steps associated with the Blockchain schema, and because of the Blockchain blocks which are linked as secure data envelopes.
16. The Blockchain block linking provides integrity to the regulatory and compliance steps.
17. The schema needs to accommodate levels of Privacy and Liability to match various financial services' needs.
18. The Blockchain encryption can secure smart contracts which are object oriented.
19. Tying financial identifiers for assets to Blockchain permissions creates a forensic trail to help prevent the same asset from fraudulently used for multiple different instruments and business uses.
20. A secure transaction model includes several essential financial components as previously identified in *Section 1* Identity Security Preface. The Blockchain encryption and Distributive Ledger can provide a security mechanism to link the financial block components as secure containers with unique legacy or open actions.

A Sample Object Oriented Secure Blockchain and Distributive Ledger Architecture

The following illustrations are a collection of activities associated with a Blockchain and Distributive Ledger. Different security entities are being presented to create an overall object of multiple layer accesses leading to an abbreviated sample transaction.

Figure 11 Distributive Ledger of this series of illustrations begins with Bank A options for Identity elements which are the basis of an encryption process that results in an e-Profile secure envelope which in itself contains sensitive information associated with protecting the Transaction. It should be noted that a Transaction process is one of many different financial services and other market usages for an e-Profile secure envelope. In the context of a financial services transaction, selected financial transaction components with their access attributes and other sensitive processes, like building an encryption key on the fly, is contained in the secure envelope. The financial components are a series of Blockchain blocks of data that are linked to a transaction. The inherent linkage is with cryptography and other identity markings associated with accepted financial services practice.

Figure 12 continues through additional figure illustrations build on an Information Collaboration Model. The model includes access attributes associated with an encryption framework like Constructive Key Management with an assignment of a designated attribute for each of the identified financial components, as well as an attribute for sharing data among a central key

Copyright 2016
All Rights Reserved

management authority. The Central Authority manages the attributes in the form of secret keys and distributes the keys with Push architecture. Other functionality exists with the Central Authority like key maintenance and other standard based functionalities for key management. In this illustration, the Central Authority is maintained by a bank. Two banks will be portrayed in support of a seller supported by one bank and of a buyer supported by another bank. At this level of the sample model are components representing compliance, audit – legal, regulator, a high net worth entity, the Buy, and the Seller. All these components are included in the current financial services use case. The communications and content technologies associated with this security architecture can change and result in a determination of which financial components are needed.

The model continues with another level of abstraction associated with the potential content of each of the financial components. An access attribute was assigned to offer access to the designated component (in this illustration) attribute 1 offers access to the BUY component). The BUY component consists of Public data, Chain details, and Transaction encryption details. The Attribute 1 is the key associated with the encrypted BUY block which includes a mix of open Public data and the necessary information pieces to decrypt the block and do other actions associated with the BUY component.

A cryptographic access capability for different access points in the overall Blockchain schema is included. The associated cryptographic engine can segregate access for a read or write or both access. This level of capability establishes differential access to a common set of information. A file could be accessed by content restriction to different persons or machines based on its access permissions through attributes. Defining these attributes are policy associated with the owner of the Central Authority Encryption administration.

Bank B is introduced into the collaborative model to cite multiple banks' applications that are associated with the Purchaser. Like Bank A, Bank B provides services to ensure the integrity of a transaction. The secure linkages and encryption of a Blockchain also ensures a chain of custody with regulatory, audit, and compliance validations.

The architecture has flexibility to structure the model so that existing legacy systems are accommodated while the object oriented block architecture can be adjusted to accommodate new ways of doing financial services.

Building a Secure Transaction Model

A Use Case is illustrated in Figure 11 in which a generic transaction takes place between a Supplier and a Purchaser with a separate bank supporting each of the two participant financial services components. The Permissioned Blockchain model of Figure 9 (Financial Service Components in the Blockchain) is modified and illustrated as a more detailed secure overview Distributive Ledger with Blockchain linkage. Limited details are included for the invoice, and for the potential use of the ISO 20022 payment schema. (Other payment schema could apply).

Copyright 2016
All Rights Reserved

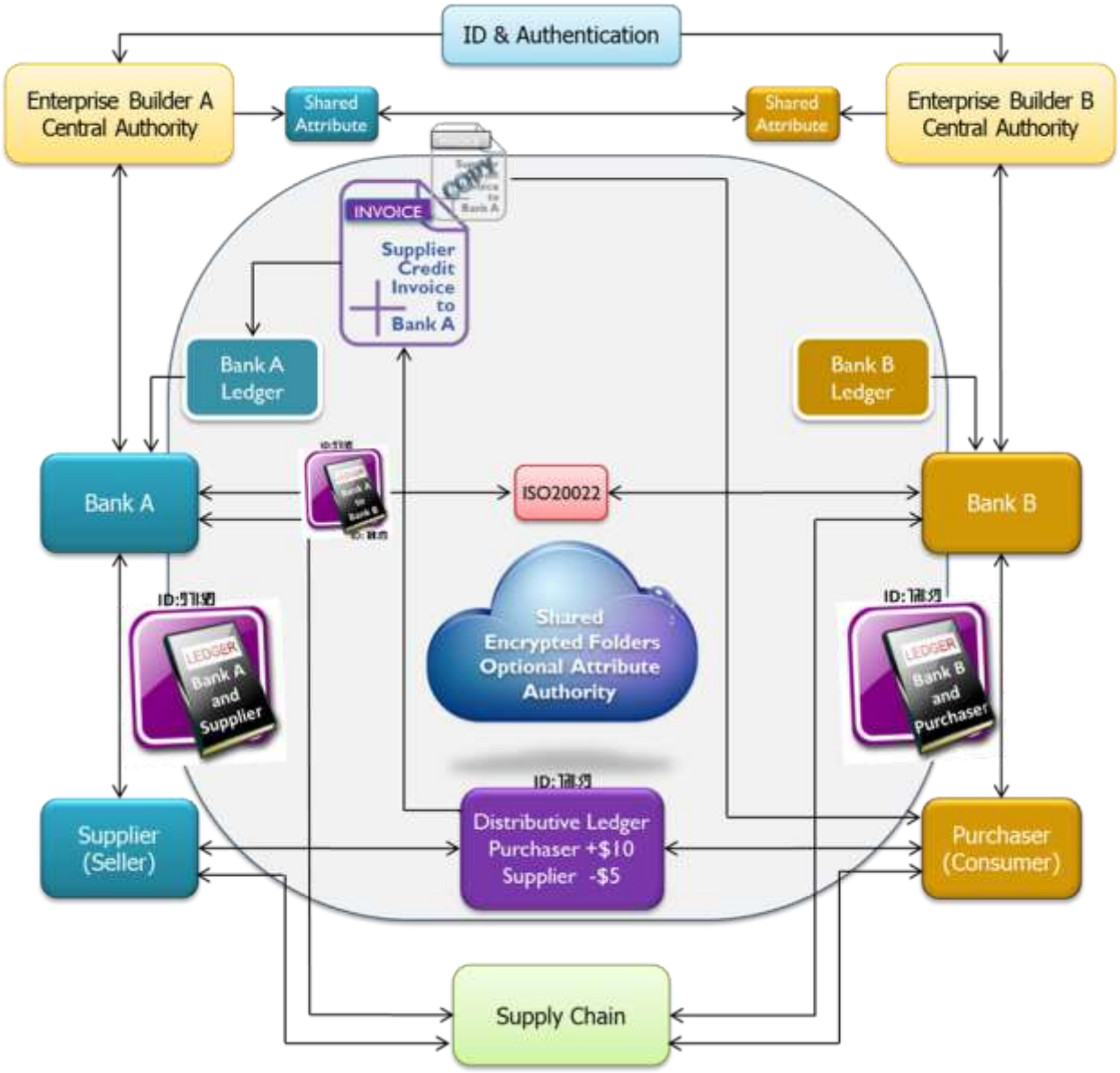

Figure 11 Distributive Ledger

A transaction can consist of two banks (Bank A and Bank B) who manage the financial accounts and related ledgers for a Supplier (seller) and for a Purchaser (Consumer). A fifth entry can be included of a merchant, but the basic model would be the same. The flow for the transaction is cited in the attachment for a central authority model in which the two banks establish Purchaser identities respectively and manage banking like today's implementations. A bank ledger exists for each bank as they relate to their respective customer, and the ledger is available on a demand basis. The attachment cites the transaction flow with attributes from Bank 1 and Bank 2, each bank would have own their separate CKM attribute access administration (Bank A Enterprise Builder and Bank B Enterprise Builder). To share attributes in this model, a Bank must share one of their attributes to others to maintain a secure sharing of data. (The encryption

Copyright 2016
All Rights Reserved

administration model includes a consideration for liability associated with managing access to the data. The example identifies two banks which would have their own administrative responsibilities. The encryption administration may be shifted to other entities other than a bank, but such an action would have to consider the liability ownership associated with the data.)

A Distributive Ledger model has the same transaction taking place but with a different security schema which includes a hybrid-CKM Blockchain capability identified in ANSI x9.73, CMS, and can be related to an object oriented protection encryption process. To do the hybrid-Blockchain capability, CKM includes a function within the CKM Combiner which can be applied to subsequent chaining actions among a transaction data flow of multiple points. In the Figure 11 example, the Purchaser wants to purchase an item from the Supplier and the Supplier needs to validate that the Purchaser has sufficient funds to pay for the item. A Distributive Ledger is established and executed among the multiple transaction points. The example model has Bank B creating an agreed Ledger with the Purchaser. (The Bank B ledger would include a unique number or identity in order to attribute the ledger to Bank B and associated with the Purchaser. The Bank B ledger would also include the amount of available funding for the Purchaser. Bank B shares the ledger with the Purchaser who now can attest to funds are available for a purchase. The Purchaser contacts the Supplier to purchase the item with funds identified in the purchaser ledger. An example can be that the purchaser begins a ledger with a $10 amount before forwarding to a supplier. The supplier deducts the amount of the purchase against the Purchaser ledger. As an example, a $5 deduction is applied against the original ledger. An encrypted Supplier invoice is created which includes internal and header data, as well as the original transaction number. The action continues with the Supplier forwarding the annotated ledger to Bank A for credit to the Supplier account, and copy of the encrypted invoice to the Purchaser for transaction receipt. The Purchaser decrypts the Supplier header only since the Purchaser would not have access to the Bank A/Suppler access attributes to decrypt the invoice (which could also contain additional Supplier proprietary data) which was also sent to Bank A. Bank A forwards the annotated ledger to Bank B to deduct the amount against the Purchaser account. It should be noted there can variations on the transaction model but the core concept would apply. To enforce the transaction cash flow and purchase flow while preventing a third party manipulation of the data, a hybrid-CKM Blockchain model can be applied. Header validation and access control can extend from a hash, a keyed hash, or an encryption framework which is identified in ANSI x9.73, CMS.

A Distributive Ledger is used by the Purchaser that identifies a validated cash amount that the Purchaser can apply against purchases, (the mechanics for establishing what the Purchaser would want to publish in a ledger may vary with policy and execution). The data associated with the ledger at this stage would be encrypted with CKM enforcement. Elements of the encryption that relate to the ledger encryption process include attributes that are associated with Bank B and the Purchaser, and a unique number for the Purchaser ledger. That ledger number would stay with the total transaction flow and be a cryptographic assurance binding for the process. (The unique number would be included within the CKM internal process to further add security integrity.)

Copyright 2016
All Rights Reserved

The encrypted Purchaser ledger number is also included in a partially encrypted Header which is part of the initial encrypted Purchaser ledger. The encrypted Purchaser ledger data includes the ledger number, the available cash amount, and other data – this becomes the first encryption step in a distributed ledger process. The encrypted Purchaser ledger is forwarded to the Supplier who decrypts the Purchaser Ledger Header and notes the confirmation of the amount available from the purchaser and the transaction's unique number. A point to consider is that the Distributive Ledger secure process may include an external identity capability as an adjunct to the CKM enforcement, or may be limited to the transaction number and URL of the Purchaser for a cash-like transaction. The next step in the Distributed Ledger process is for the Supplier to get credit for the transaction by forwarding the original encrypted Purchaser ledger with its CKM enforcement Header which is encrypted with the Supplier CKM attributes and the purchaser unique identity number, the resultant Supplier Header with the encryption includes the plaintext original identity number and the Supplier's transaction cost. The double secure encryption wrapped transaction is used by Bank A to credit the Supplier account by decrypting the Supplier CKM-Header to establish the credited amount. Bank A confirms the transaction and settles the $5 debit against the Purchaser account with a Bank A encryption of the multiple encrypted Distributed Ledger originated with the Purchaser and continuing through the secure transaction process.

A two or more bank model approximates existing financial services. A faster transaction model could leverage fewer entries beyond the Purchaser and Supplier entries. However, to accommodate the existing regulatory financial transaction infrastructure, several other financial services components must be considered beyond the Central Authority component of a bank, the Purchaser component, and the Seller component. The Regulators, the Auditors, and Compliance components complete the transaction process.

The Distributed Ledger is a digital form of a financial transaction. The encryption process is a digital form. Identity may be a mix of analog and digital functionalities. The partially encrypted CKM Header offers a performance advantage to track the transaction while including encryption – the encrypted ledger does not have to be decrypted during the transaction processes but its encrypted data provides a multiple step access which can be validated by a third party with proper access encryption attributes. Only a bank in this example can provide the proper access encryption attributes. Fraud is minimized since the encrypted transaction requires access through two levels of decryption – one decryption for the header associated with an entities action and one decryption for the transaction ledger. The amount identified in the header must match the encrypted amount contained in the Ledger. A Compliance CKM attribute can be added to each encryption step in the secure transaction – the attribute would be unique to a compliance action and be managed by the compliance entity for a third party validation.

A faster payment transaction may take a different form of a distributive ledger in that the object oriented protection encryption schema can create a security state that permits an extended time before a transaction needs validation. The current security validation per transaction event adds time to a transaction validation. Validation between the two banks of the above transaction

Copyright 2016
All Rights Reserved

process for each transaction adds a defined time to a Distributive Ledger model. A minimum time frame can be established between two parties to a transaction: the purchaser and the seller. However, both parties want an assurance that funding is available for a purchase, and that the funding can be captured by the seller. With the addition of a CKM object oriented framework, Bank B of the Purchaser establishes a certified account which the purchaser can draw against. At that point, the Purchaser has a defined amount of currency to apply for use. The Purchaser establishes a transaction with the seller to buy pencils. Like the generic transaction model, the action of the seller is the same. A seller invoice is created identifying the amount deducted from the purchaser's currency/consumer Ledger and forwarded to the seller's Bank A and the Purchaser. The purchaser knows that the seller will be sending his pencils and has deducted the money from the certified Purchaser's ledger. The bank to bank reconciliation of this transaction would not be done at this time but established by policy (agreed upon of how often should a collection of transactions be validated between banks). By having an encryption overlay at the data object level, and having an encryption hybrid-blockchain among the transaction process, the bank to bank reconciliation may be extended for several days. The result is to increase to a faster payment – transaction process without compromising security and maintaining legacy systems to the extent possible.

Details of a Secure Blockchain Distributive Ledger Use Case

A Secure Cloud Environment

Financial Services are using various communications channels such as the Internet and private rails to execute transactions and payments. Other services are also available through these channels.

Collaboration, information sharing, and anywhere, anytime, anyplace, any-device access to information are all terms discussed daily by companies as they try to find ways to increase efficiencies, cut costs, and effectively exchange critical-business information with their trading partners, suppliers, employees, and their extended value chain.

In addition to the financial services communications channels and the information sought by companies, is the use of cloud services. These security services must include technical controls for encryption of data at rest, of data in transit, and other data audit-handling compliance requirements. Compliance may call for specific levels and granularities of audit logging, other financial security components are also present such as legal (court) and regulatory components. These components can result in the generation of alerts, activity reporting, and data retention. As an example, a data owner which is subscribing to a cloud has provided their own data assurance or contracted for an identified level of data assurance protection. The cloud may be viewed as a meeting place for collaboration beyond only a storage service.

Copyright 2016
All Rights Reserved

A Sample Online Cloud Access Control Use Case Enforced by Encryption

The use case is an online cloud model like a cloud service which can do full trading partner participation for a supplier and purchaser and their banks as seen in Figure 12. A Supply Chain is identified to accommodate the logistics associated with the sale of material.

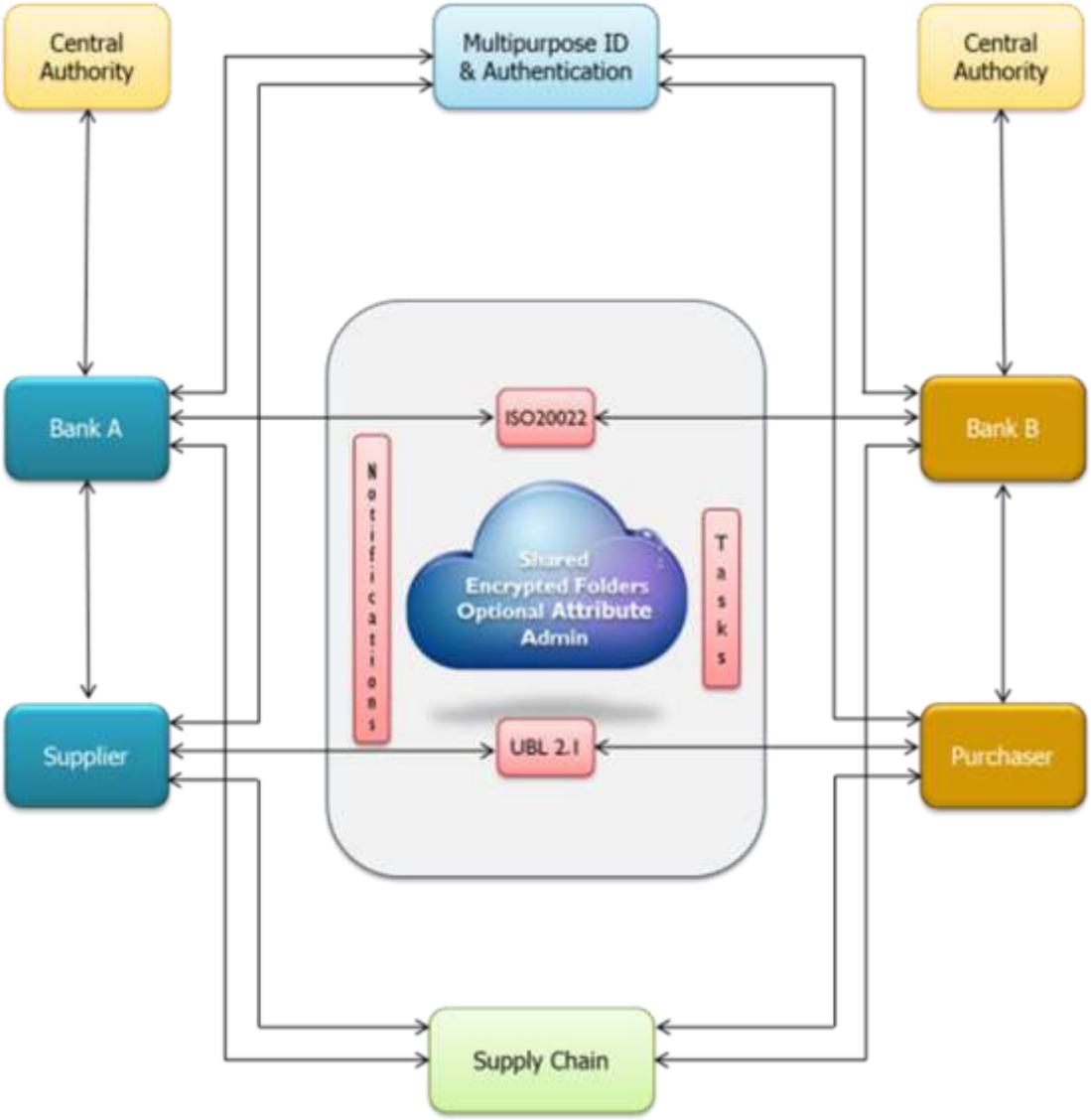

Figure 12 Information Collaboration Model

To reach a broad participation with the overall capability, the cloud services could provide a range of support for file and message services with selective encryption service. Granular access and granular protection may be the goal for the files and messages that can be shared among participating banks and the participating supplier and purchaser. A hierarchical folder structure could be used for organizing information including information that has been encrypted. Applying a shared folder space between two collaborating parties, content sharing is possible through the metadata of the encrypted information. The shared folder may be considered similar

Copyright 2016
All Rights Reserved

to a publish/subscribe metaphor. Once the use case for information storage and sharing is established, the encryption process could be applied to a Attribute at the data or message level as described in ANSI x9.73 CMS for Constructive Key Management.

Attributes may be identified with roles or with rules in the context of access control with encryption enforcement. The encryption split key associated with an attribute needs to be held confidential, but the attribute nomenclature may be identified in the public domain. (An exception could be if Traffic Analysis requires both the encryption split key and the associated attribute nomenclature be confidential.) The attribute nomenclature may be identified within an application by limiting the attribute to a numbered content identity reference aligned from a financial services attribute listing, or, the attributes may be identified by the attribute nomenclature from a financial service attribute listing.

Mathematically, a Boolean logic relationship can be established between Attributes such as a Logic OR or a Logic AND.

- A Logic OR would have either Attribute for two attributes applicable, or a Logic AND would require both attributes.
- A Logic OR may be considered as expanding access control; whereas, a Logic AND may be considered as contracting access control.

Table 3 Attribute Labeling

A Use Case Sample Label/Attribute/Attribute Listing	
Purchaser	Attribute 1
Supplier	Attribute 2
High Net Worth Entry	Attribute 3
Compliance	Attribute 4
Application Access Control	Attribute 5
Regulator	Attribute 6
Auditor	Attribute 7

The management of the attributes and other encryption parts is with a Central Authority. The Central Authority, in this use case, is controlled by the banks. The Central Authority may be financial services in which a bank or other financial service entity licenses.

To begin as a transaction example, consider an event for a given Folder based on an invoice and a transaction. If a customer has created a payment folder and associated a service provided payment policy to it, the user could drag a newly arrived invoice into the Payment folder resulting in an event which would be propagated to the payment service. The payment service would retrieve the invoice and transform it into an XML payment document. The payment service would then send the payment document to the bank for transferring the appropriate funds to the supplier company that generated the invoice. Identity policy and components could be established for each bank. Further digital logic can be applied to align the collaboration process to a financial services business case.

Copyright 2016
All Rights Reserved

Metadata descriptors are important for sharing and establishing secure access. The metadata packet was discussed earlier in the document. Access policies are an integral part of the information itself and travel with the information in such a manner that information can be present anywhere, anytime, anyplace, and on any-device. Moreover, protecting the data ensures confidentiality of the information being exchanged between two or more collaborating entities. Role or rule based control can establish a conformance to the information flow which was intended through the hierarchical folders.

The supplier and the purchaser must have an appropriate encryption keying material. Establishing a model for sharing data once encrypted is done with an attribute administration. When establishing the hierarchical folders, CKM encryption attributes are established based on information identity criteria found in the financial service attribute listing. Identity can be established through roles, rules, and other characteristics for classifying information or data. Additional identities can be established as a separate process of multiple purpose ID and authentication with an Identity Security model as previously discussed. These attributes come with CKM keying material and have a key management framework to comply with other ANSI and other cryptographic handling standards.

The encryption schema of metadata and encrypted data can be viewed as an object container which can include additional object containers to provide distributive, compartmented separation of secure information access within a common file or common message. Encrypted/coded data can be displayed as redacted information in a usable format. Secure containers can be established for selected financial service components and nested as an independent secure container within a Blockchain object container linking the containers with nesting. With a mix of attributes that are different among the object containers, a single object container can have selective access for different financial components or further granularity with segments of information such as tiered access to pieces of invoice data – the multi-carbon paper used in the past left different levels of access for a paper solution. The object container can be viewed as a digital representation.

Encryption key components for protecting the content in this use case can be directly aligned with information control dictates. Since the key components are directly associated with information control such as roles or rules, a few key components may only be needed. The resultant encrypting keys, for which the key components are in part, include a random capability to ensure that each encryption message or encrypted information is unique and protected. The key management administration maintains the distribution and integrity of the component keys and other criteria supporting the encryption framework.

Figure 13 illustrates the basic collaboration entities which can be related to a simple supplier and purchaser exchange and transaction (additional actions are possible):

- Purchaser requests for pens from Supplier
- Supplier confirms with invoice to Purchaser
- Purchaser pays invoice through its Bank B

Copyright 2016
All Rights Reserved

- Bank B confirms payment with Supplier Bank A
- Bank A confirms with Supplier that funds are available
- Supplier sends pencils and confirms transaction

The following is a sample Attribute exchange example among Purchaser, Supplier, Bank A, and Bank B:

- Bank B issues Attribute 1 between Bank B and Purchaser
- Bank B exchanges Attribute 1 to Bank A to establish use with Supplier (sensitivity and/or privacy of Purchaser has established a need to protect details for purchase and transaction details)
- Bank A establishes a crypto relationship between Bank A and Supplier with Attribute 2, and exchanges Attribute 2 with Bank B. (The Supplier Attribute 2 can be used to protect details of the invoice).
- A transaction confirmation can be achieved by combining Attribute 1 with a logic AND to Attribute 2.
- The Purchaser may be considered a high net worth entry and have a separate Attribute 3 to further protect its identity and/or privacy during a transaction.
- A company may have a compliance rule application for which the company would want to maintain usage with encryption enforcement through Attribute 4.
- Encryption can be used to provide enforcement to a component application or a component message within a container-like message with Attribute 5.

To complement the collaboration process includes an example of a financial services messaging exchange process through ISO 20022 (or other payment schema) and the Universal Business Language (UBL) for a supply chain interchange. XML is a coding schema for ISO 20022.

ISO 20022 messages are available for the complete end-to-end payments chain:

- Customer-to-bank (payment)
- Bank-to-bank (payment clearing and settlement)
- Reporting (cash management)

The messages can be encrypted with the access controls and Attributes previously identified.

ISO 20022, UBL, and XML are examples only to illustrate a financial service's payments architecture, but other payment schema may be used with the encryption.

Secure Payment Transaction Process

Overview of an Information Collaboration Model

The banking industry has a reliable, robust financial transaction transport infrastructure in place. Protection of the transaction process relies upon trusted connections between supplier, purchaser and banks. Spectacularly successful attacks are perpetrated against these primary data stores simply because sitting there, unprotected, rests the high value return on investment treasure.

Copyright 2016
All Rights Reserved

The flow of financial data through the transport infrastructure has experienced attacks centered on denial of service more than data theft. It is only a matter of time before data traversing the financial infrastructure will increasingly become the focus of possibly undetectable siphoning.

The advantages of an information collaboration model to cryptographic enforcement of policy and data protection is derived from encrypting the data package without modification to the transport infrastructure or data headers. This approach makes the mechanism independent of transport protocols and provides low to no impact on data infrastructure legacy investments. Financial transactions between entities have the data package wrapped with unique encryption attributes known only to the entities involved. These can only be decrypted by those entities in the transaction path which have shared attributes thereby achieving a mechanism of persistent data binding to identity and authorization attributes, seamlessly maintained from initialization to storage.

The Information collaboration model standards based technology is applicable to the banking industry for protecting financial transaction and data storage. The bank's existing services are enhanced by the addition of the Model. The model enables the use of cryptographic attributes created and controlled by the bank to compliment unique Identity and Authorization (I&A) capabilities for the bank and its customer. It is possible for the customer's attribute be imbedded in a bank card given to the customer and applied through the model's protocols to all customer account data as it is created and stored. Using a single persistent protection schema, banks, customers, and their data are protected from compromise during the transit and storage of sensitive financial data. Should compromise be accomplished, the attacker's access is confined to one individual account having compromised only that customer unique attribute key protecting their data. The intent is for no data breach of the institution's entire data store.

The same model's technology can also be used for Bank-to-Bank financial transfers.

The following is a series of illustrations which build a use case for the Information Collaboration Model of Figure 12. The illustrations begin with Figure 13 Unencrypted Data Moving Through a Financial System. The illustrations include commentary to reinforce an action's flow.

Copyright 2016
All Rights Reserved

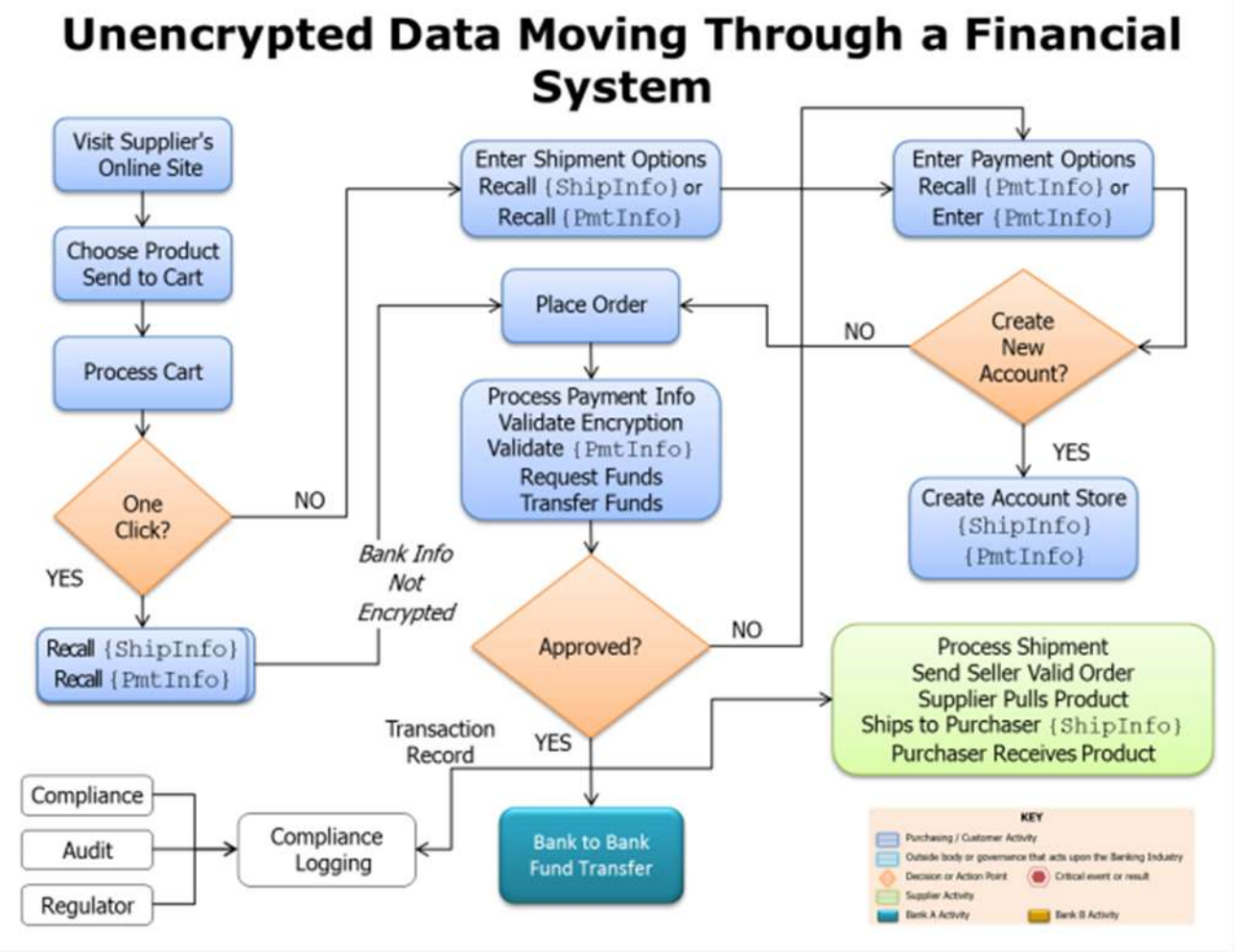

Figure 13 Unencrypted Data Moving Through a Financial System

Copyright 2016
All Rights Reserved

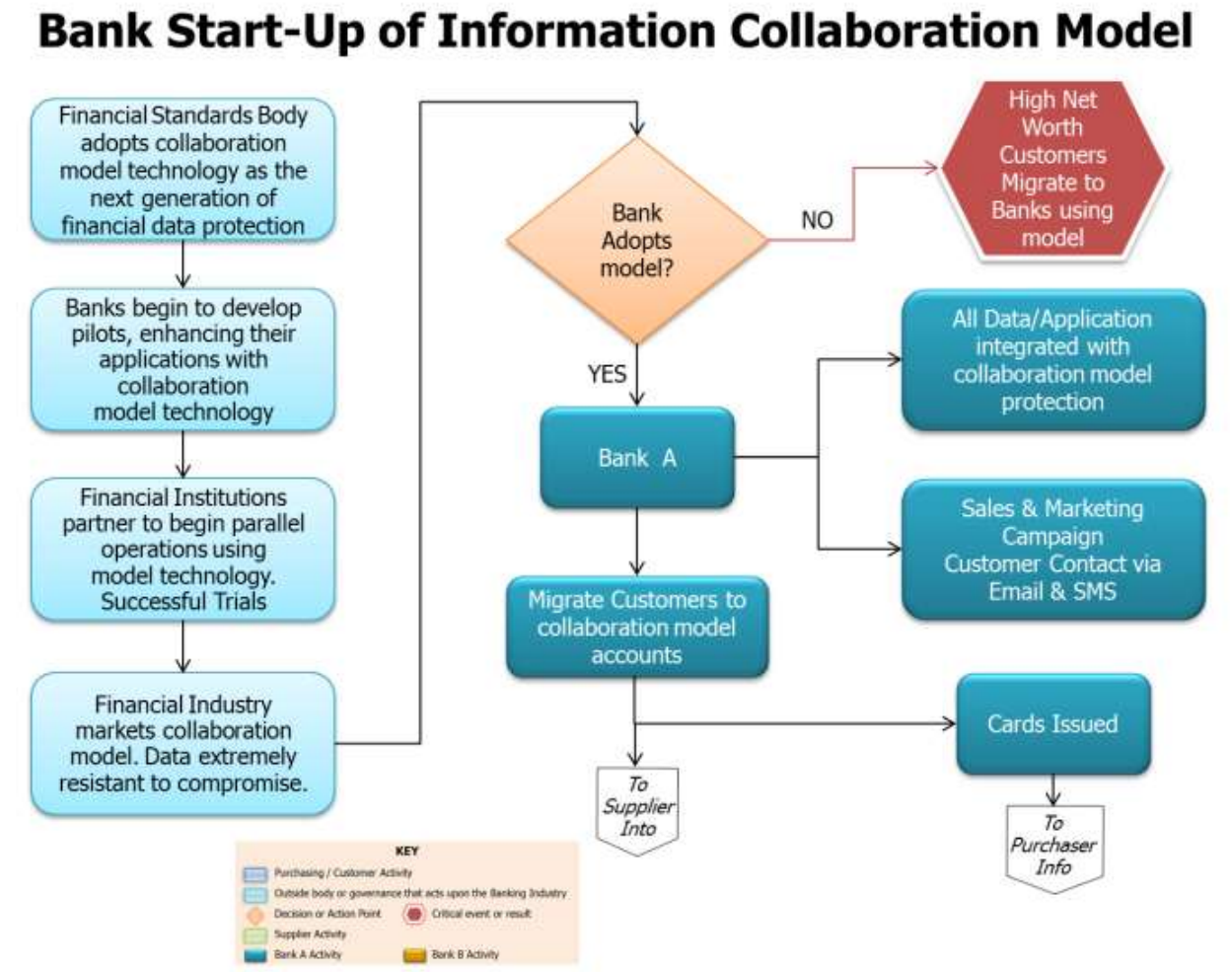

Figure 14 Bank Start-Up of Information Collaboration Model

Copyright 2016
All Rights Reserved

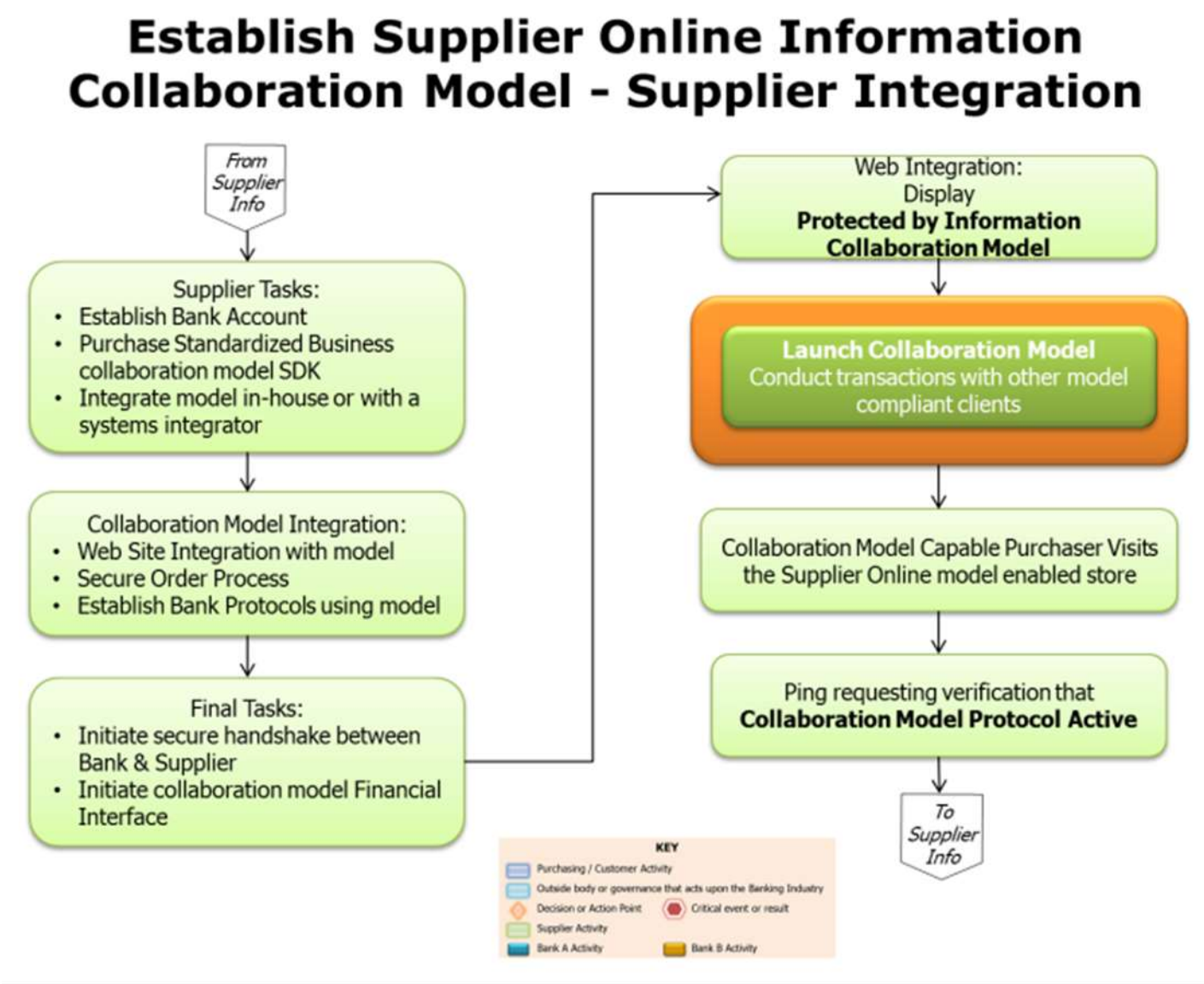

Figure 15 Establish Supplier Online Information Collaboration Model

Copyright 2016
All Rights Reserved

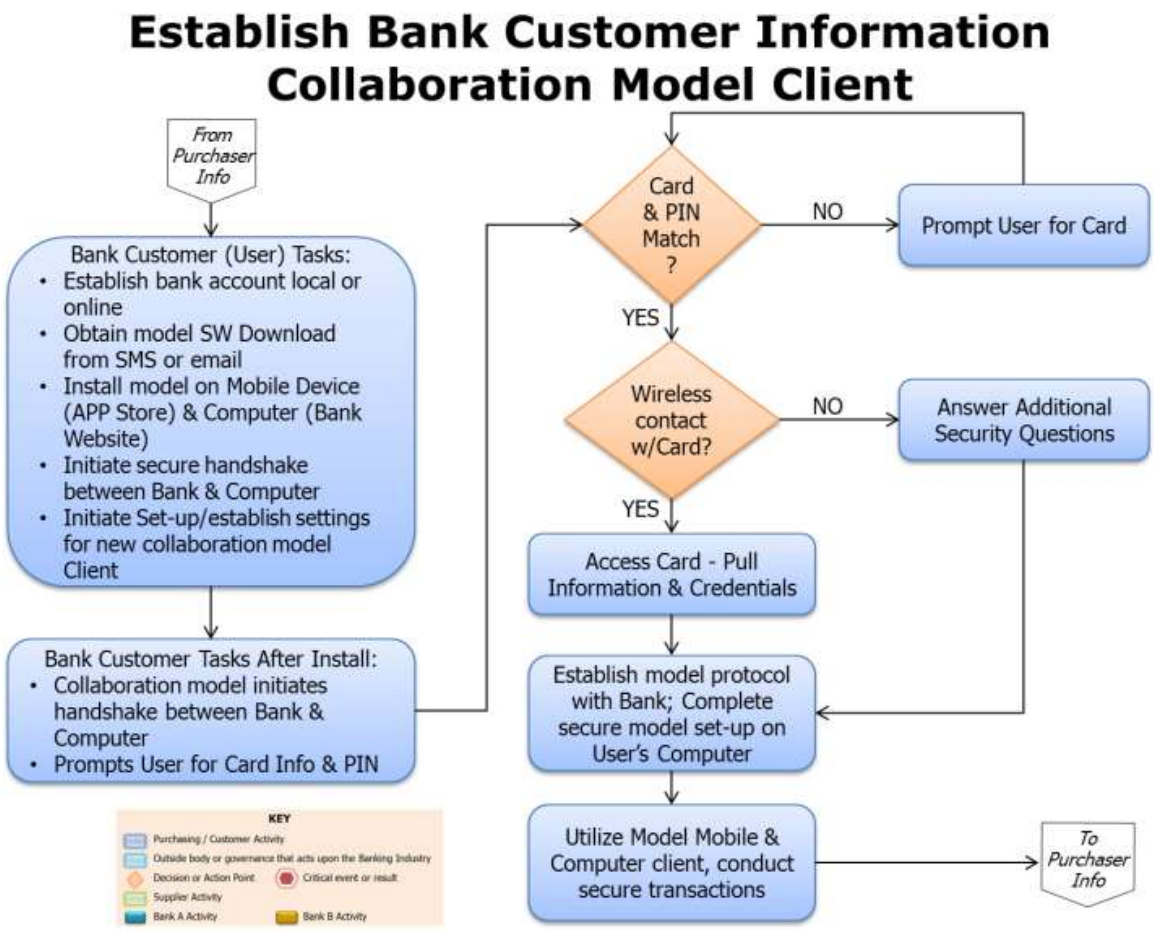

Figure 16 Establish Bank Customer Information Collaboration Model Client

Copyright 2016
All Rights Reserved

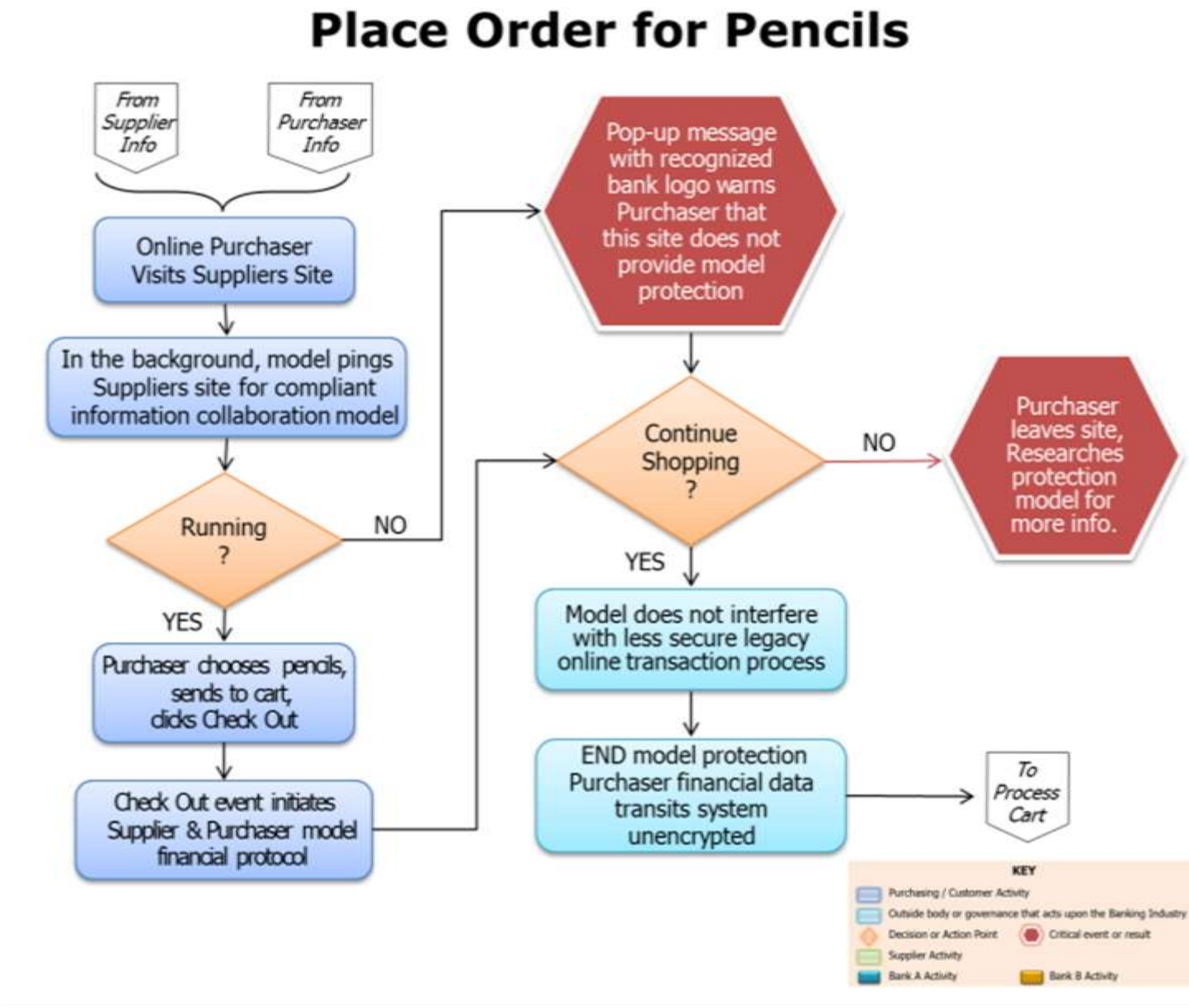

Figure 17 Order Placement

Copyright 2016
All Rights Reserved

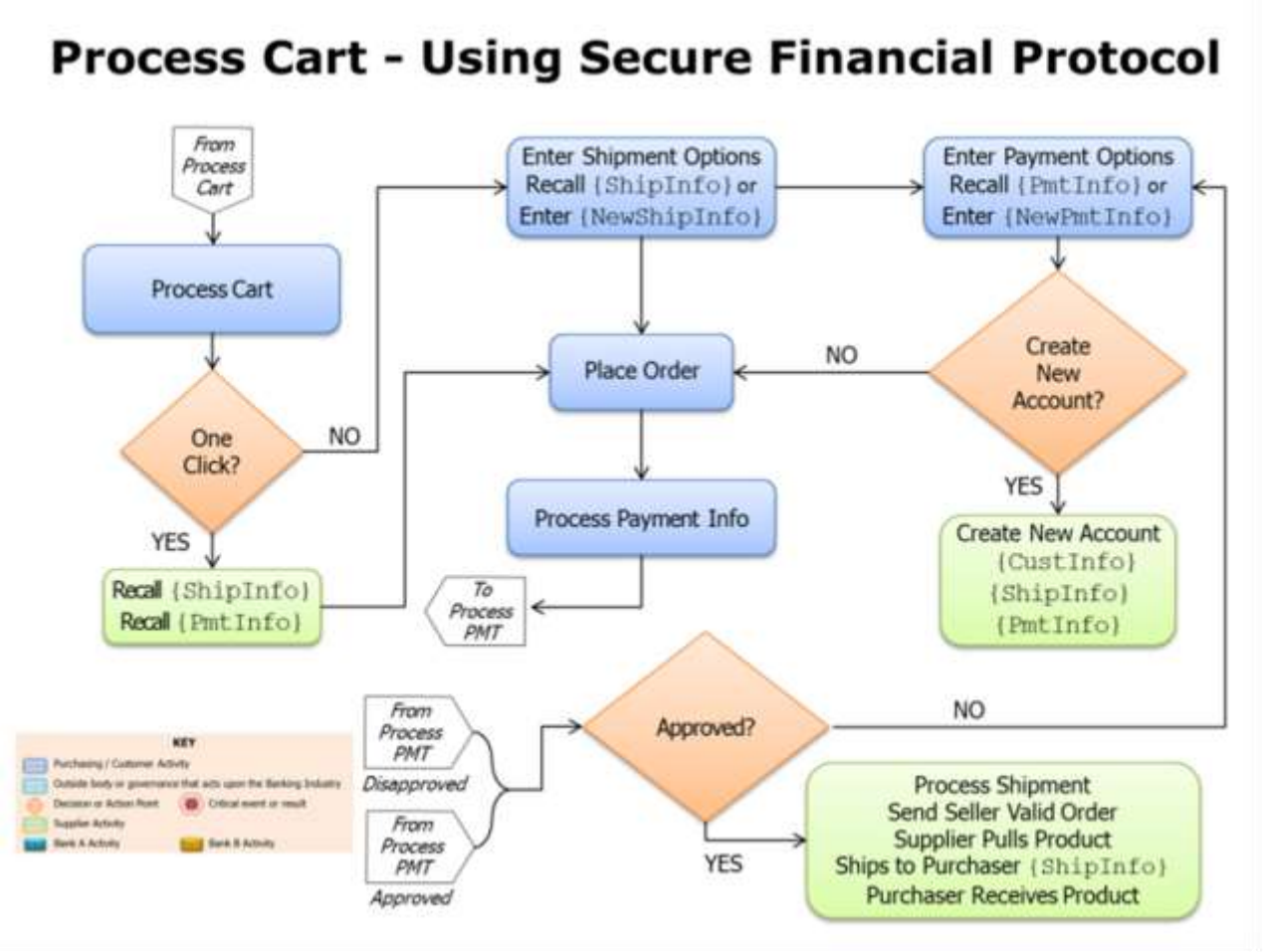

Figure 18 Process Cart Using Secure Financial Protocol

An encryption process in Figure 18 is applied to the transaction which includes selected attributes.

Copyright 2016
All Rights Reserved

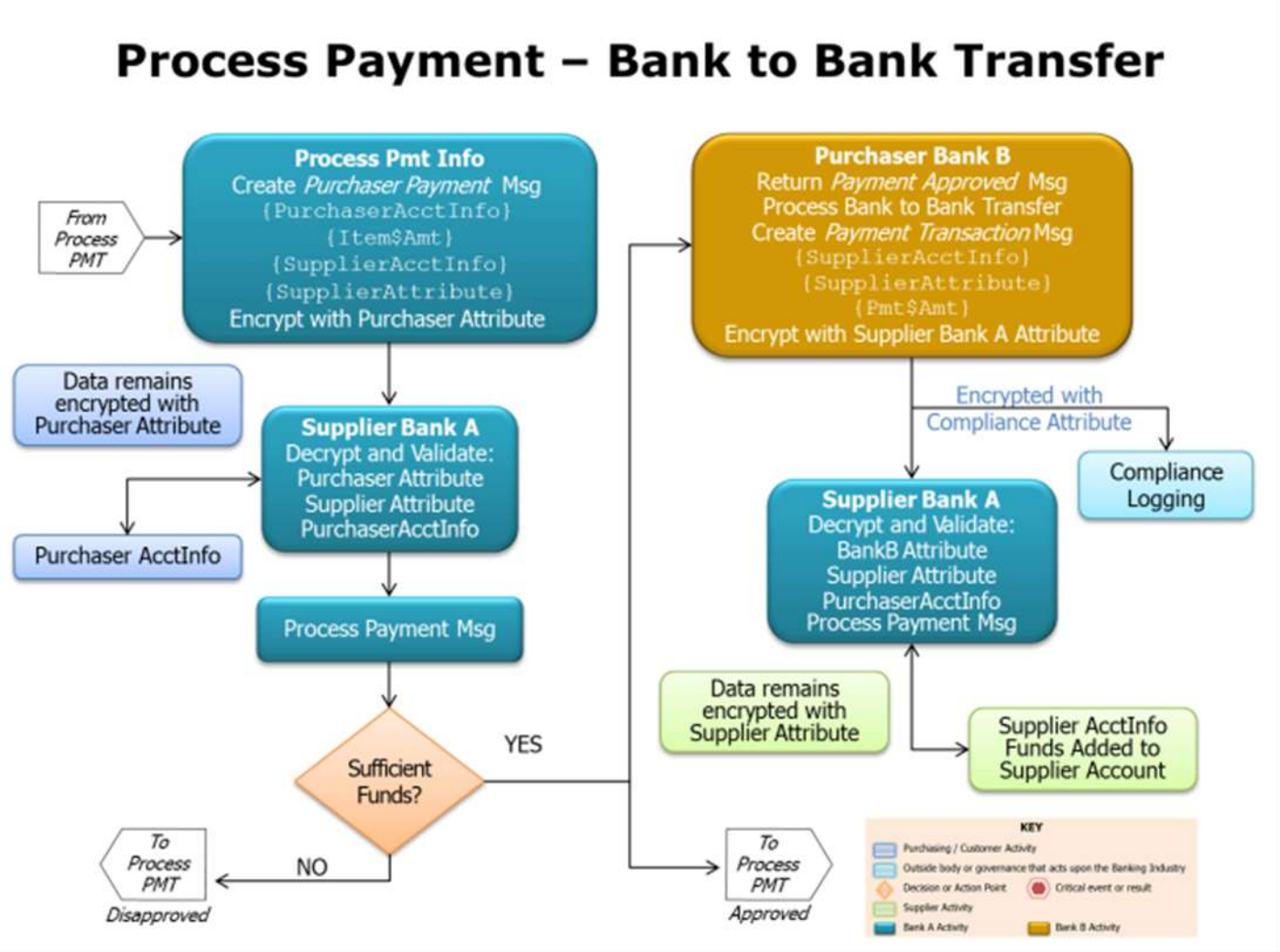

Figure 19 Process Payment – Bank to Bank Transfer

The transaction data is encrypted and can be distributed and stored in formats like the cloud. Other steps associated with a transaction can also include levels of access control with encryption enforcement. A business model can be established which includes what roles should identity security encompass as well as what overall security profile is needed.

A secure transaction can be viewed as a financial services event which must include what that financial security has established as it security profile. Legacy security models exist which would need to be included with a further notion that protecting at the data object level will entail an implementation process which enhances existing security. A network security profile that relies on perimeter defenses will need to also include a migration to protecting data.

Copyright 2016
All Rights Reserved

Annex A. Setting the Security Stage

Over the past several years, we have witnessed the Internet, and related technologies, significantly change the complexion of distributed computing environments into a fundamental aspect of one's existence. A similar transformation has been taking place with security. A picture of a secure enterprise can now consist of different categories defined as: Network Security, Device Security, and Information Security. Figure 20 Enterprise Security Categories illustrates each of these security categories and their roles.

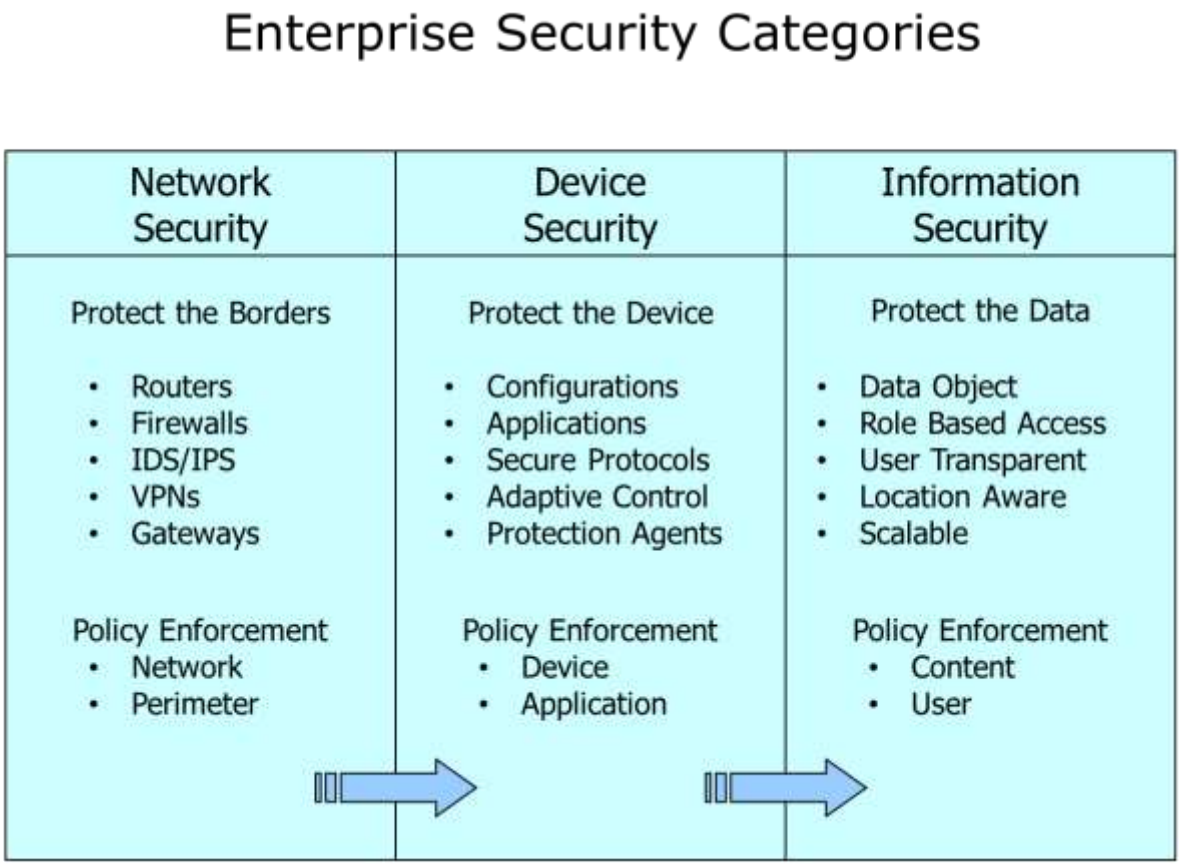

Figure 20 Enterprise Security Categories

Attacks and threats have appeared in each security category. An example of a threat in the Network Security area would be the Distributed Denial of Service (DDOS). A threat example for the Device Security is malware. And, finally an example of a threat to Information Security is an attack on data. Common among the various protections are the control of access as well as providing confidentiality to the information within each of the categories being protected.

Encryption has emerged as a security tool which can augment security policy within these various security categories. The mathematics of encryption provides a basis for a high assurance to ensure a process is executed as stated.

Over the years encryption has had periodic advancements:

Copyright 2016
All Rights Reserved

- As a general form of providing confidentiality to information,
- As a digital signature for linking an action to an application and a bridge between an action entity and the application,
- As an access enforcement for the information as an object,
- As an inherent process in a portable hardware token which protects access to the token device, and
- As a bridge among nested applications to ensure application and data separation.

Encryption can be included in various use cases:

- Identity is a category of security. Different factors can be defined under identity. A biometric event, a password or a PIN, or a token have been used in identity applications. A biometric, such a voice representing an individual, is an example of an identity factor. In this example, encryption can bind the voice biometric to an authorization thereby limiting access to a specific individual or device. Another factor can be the creation of a password with an encryption technique. Finally, one or more identity factors can be used under a policy which becomes input into an encryption process. The resultant encryption process further protects data as a collective identity for access to private information (or data).
- Protecting and providing confidentiality to content (information or data) through encryption is another important category of security. Differential access to content is an encryption technique that can apply for use cases. An example might be found within common content such as a file which can contain various users, but differential access can be achieved granting access limits to the various users through a use-policy enforced with encryption. As an added dimension to a persistent enforcement, encryption can bridge identity, authorization, access control, and protect data in a collected action.
- Privacy and Liability can contain security issues for the business usage. To prevent or to minimize the impact of a privacy issue or of a liability issue, encryption can be exhibited in one or more roles such as identity enforcer, as an electronic signature, or as an authorization for limiting access to a specific action. Each role can be modeled to reinforce the legal objective defined under privacy or as a liability shield.
- Protecting the application process with encryption access control can be another security layer.

A larger security picture emerges that builds on the financial services.

Copyright 2016
All Rights Reserved

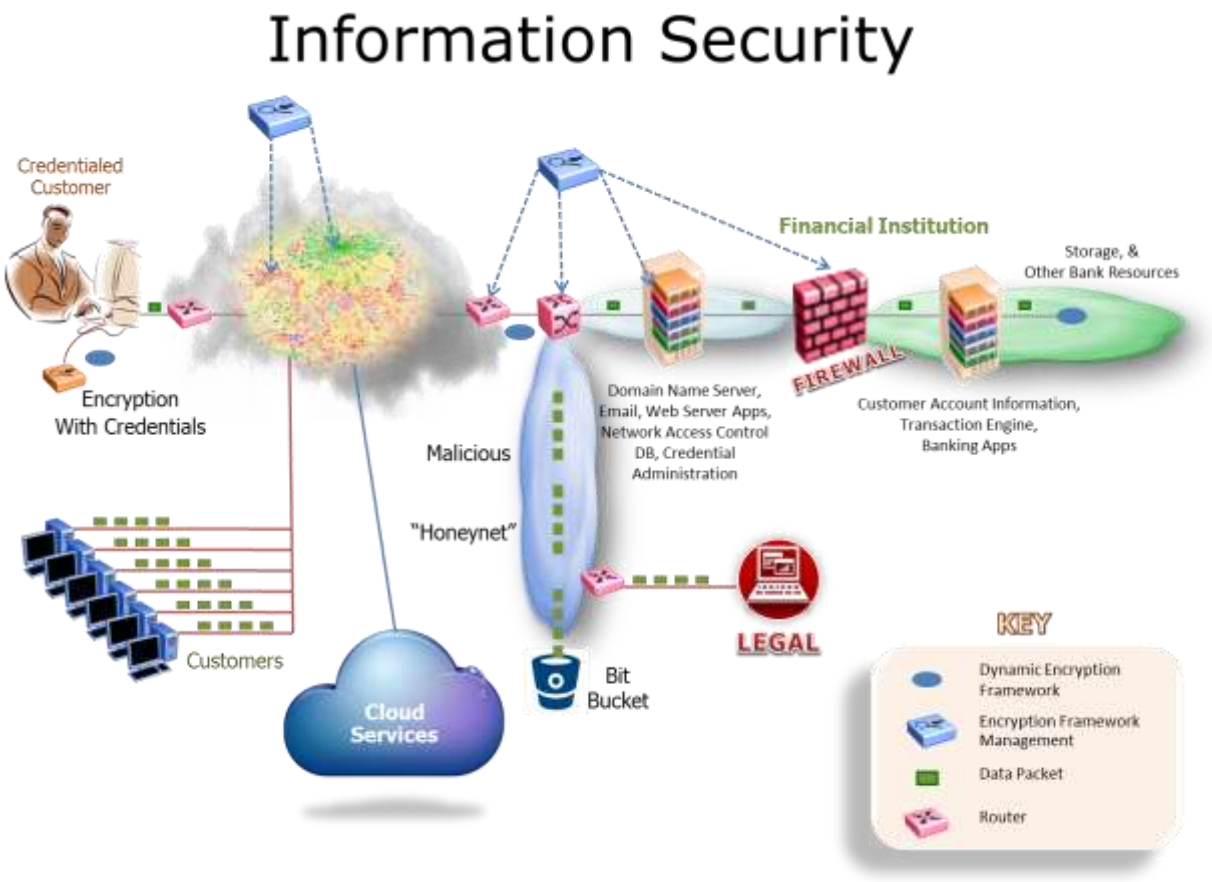

Figure 21 End to End Security Infrastructure

Figure 21 illustrates an end-to-end security infrastructure which includes financial service security components. The security framework can accommodate a financial service customer or a bank-to-bank content sharing. The infrastructure would include security tools such as routers, firewall, and encryption key management administration. The infrastructure can include a malicious Honeynet compartment for data that would be further handled separately from the main financial services process. Data can be tagged through an encryption header or non-encrypted metadata to provide differentiation to what is acceptable for further legitimate processing.

Applying encryption can be based on standards. Encryption paradigms appear in ANSI x9 standards, in the standards of the International Organization for Standardization (ISO), government bodies such as NIST, and an assortment of other standards bodies.

Within the x9 standards is the Cryptographic Message Syntax – ASN.1 and XML which defines various cryptographic capabilities and methodologies that can be applied to a financial services use case. To apply cryptography within a use case, an understanding of an encryption framework will be needed. The fundamentals of an encryption framework include the management and life cycle of encryption keys (an essential part of cryptography which is usually

Copyright 2016
All Rights Reserved

treated as secret). Differences in the mathematic makeup of encryption frameworks offer models which can be better suited for specific use cases.

A Certificate Authority can apply to a digital signature use case. A signature framework can be applied to various content types. The cryptographic message syntax further identifies Enveloped Data which, in short, has content encrypted under a symmetric content-encryption key (CEK), and the CEK is, in turn, encrypted under each recipient's public key or a shared symmetric key, and included in the key management information. A hybrid key management and encryption framework under Enveloped Data is Constructive Key Management (CKM). Components of keying material, both symmetric and asymmetric type of keys, are combined together using a mathematical function to produce an object key. The asymmetric key components are associated *with labels or credentials* which may be viewed as information identifiers, as roles, or as rules. An action with a credential may give access to a process, or access to a use case application, or a more granular differential access with component related labels, or enforce a policy associated with access to a user case application. Once the object key (or a working key) has been created and used with an encryption algorithm such as AES, the encrypted data and a related metadata header can be viewed as ready to complete a user case action. The action of creating an object key for every use creates a dynamic key operation. Once the object key has been used, the object key is not reusable and is erased. Annex D includes further details associated with CKM.

Many use case applications can be derived from the encryption schema and frameworks identified in Annex D. Security with cryptography is always changing to adapt to the financial services market needs and business models. History has illustrated changes in what can be defined as enterprise security categories. Addition and shifting has been taking place from a Network Security category, to a Device Security category, and currently to the Information Security Category.

Copyright 2016
All Rights Reserved

Annex B. Defining Objects for a Currency

Financial services have a long history of representing currencies as physical objects. In some business situations, digital representations are being used for payments and transactions, but the digital references are limited to identifying a currency. In 2015, the financial services industry has begun to discuss in earnest if, and how, a currency can have a digital representation managing specific objects associated with a currency. The objects can be addressed as data aware objects or smart objects that are data label aware. Technology exists for a security architecture that can be applied directly to the identified objects. Leveraging ISO and TC68 standards may be a basis for going forward with identifying what constitutes objects within a currency, and how these objects may be used to promote digital application usage.

Objects as Units of Information

A digital object is an abstraction that can refer to any type of information. An object may be considered a unit of information that includes properties (attributes or characteristics of the object) and may also include methods (means of performing operations on the object). The object may be simple or complex, ranging from values used in databases, to graphics and sounds. In addition to the data that makes up the fundamental content, the object often includes metadata that describes the resource in a manner that supports administration, access, or preservation.

Objects can be defined through previous representations which can be found in physical correspondence and in a digital representation found in ISO 20022. Both of these are discussed below.

Objects within Correspondence

Figure 22 Objects within Correspondence illustrates an example of a collection of identified objects which are contained in a business piece of physical correspondence – an envelope. The objects are subjects associated with the United States postal guidelines for mailing an envelope. The correctness of each of the objects ensures the correct delivery of the correspondence.

Copyright 2016
All Rights Reserved

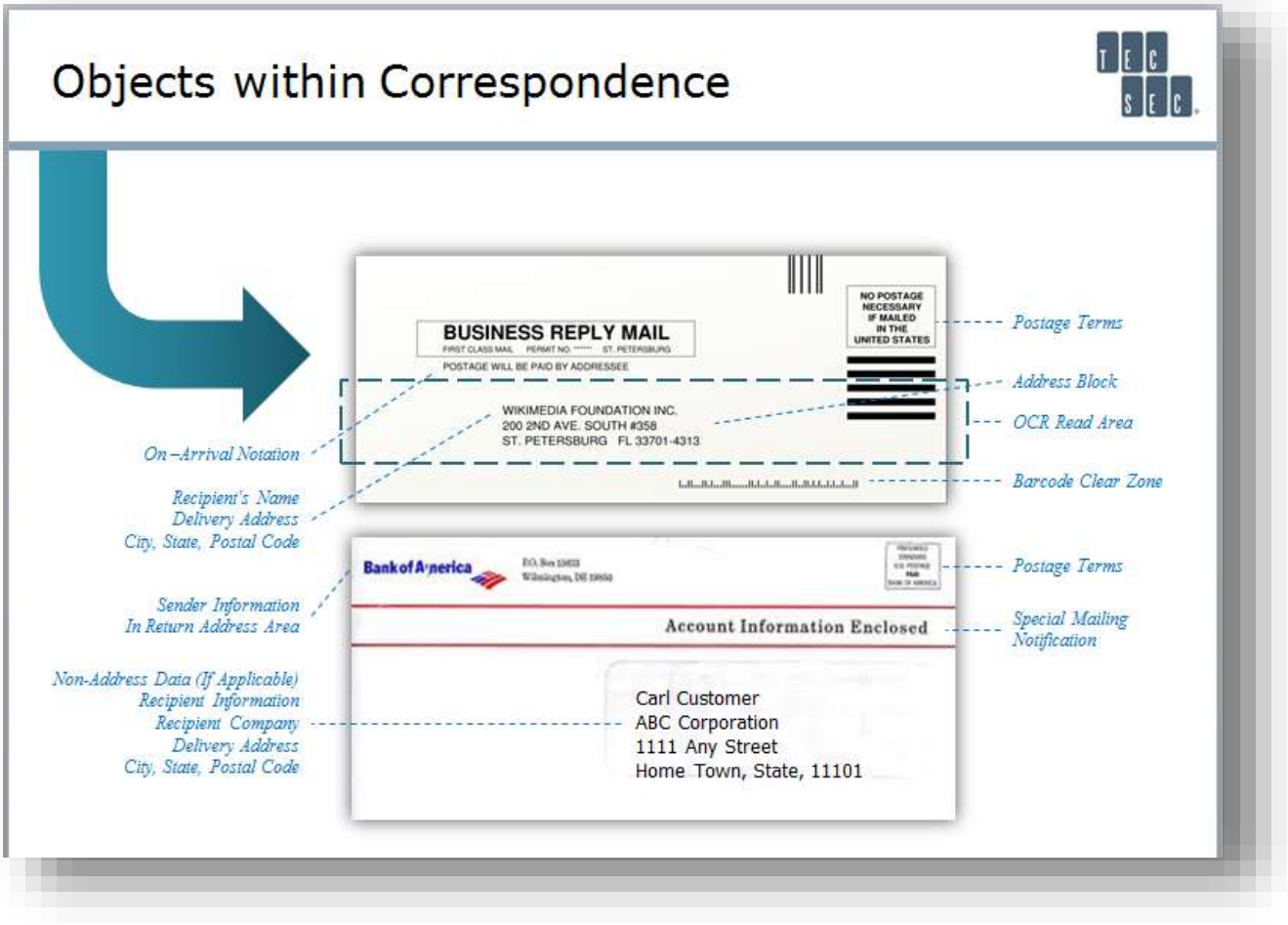

Figure 22 Objects within Correspondence

Objects Identified with an International Payment Schema

Objects representing information and data have been standardized. An example of leveraging objects in a digital format can be seen in the ISO 20022 standard. Note that the 20022 methodology follows the concept found for physical representations in that ISO components are treated as objects and identify the necessary collection of components to constitute a payment message or a financial transaction.

In the ISO context, the standard describes the agreement on what information is expressed, while the syntax is the format or the *language* used to express that information. A message definition provides a clear classification of the information and data formats (field lengths, codes, character sets) that can be exchanged between parties and can be looked at logically as a description of what data is exchanged in the message, its structure, and what it means. These logical definitions can be mapped to the business definitions defined in ISO 20022. Although ISO does not dictate the syntax of the messages, XML is the most widely used syntax for message specifications, currently, and XML message schemas are derived from the ISO UML message models.

Copyright 2016
All Rights Reserved

ISO 20022 messages are available for the complete end-to-end payments chain: customer-to-bank (payment), bank-to-bank (payment clearing and settlement), and reporting (cash management). These financial message definitions are divided into business areas (these are well-recognized functional domains in the industry) and are identified by business area codes (4 characters). These codes are:

- acmt – Account Management
- admi – Administration
- caaa – Acceptor to Acquirer Card Transactions
- camt – Cash Management
- catm – Terminal Management
- pacs – Payments Clearing & Settlement
- pain – Payments Initiation
- reda – Reference Data
- seev – Securities Events
- semt – Securities Management
- sese – Securities Settlement
- setr – Securities Trade
- trea – Treasury
- tsmt – Trade Services Management
- tsin – Trade Services Initiation

The message flows that represent a particular business transaction comprise messages from the business areas defined above. For example, a customer-initiated direct debit initiation message (pain.008.001.03) will result in a customer payment status report message (pain.002.001.04). Full details of the message flows for all business areas can be found in the ISO Payments Messages (see Resources) section of the ISO 20022 website.

Objects within a Financial Instrument

Figure 23 Objects within a Financial Instrument illustrates a bridge between physical financial instruments in which objects have been identified. The bank check with its defined objects can be further linked to a virtual environment through its data objects (the whole check can be represented as a digital graphic). Like the envelope, the check contains these objects to enable a correct banking action, such as a deposit of funds. Each object, like the Routing and Transit Number (RTN), may be treated in an independent role, and subsequently used in a collective database – in essence, a data object can have more than one usage; whereas the check itself may be limited to a single role.

Copyright 2016
All Rights Reserved

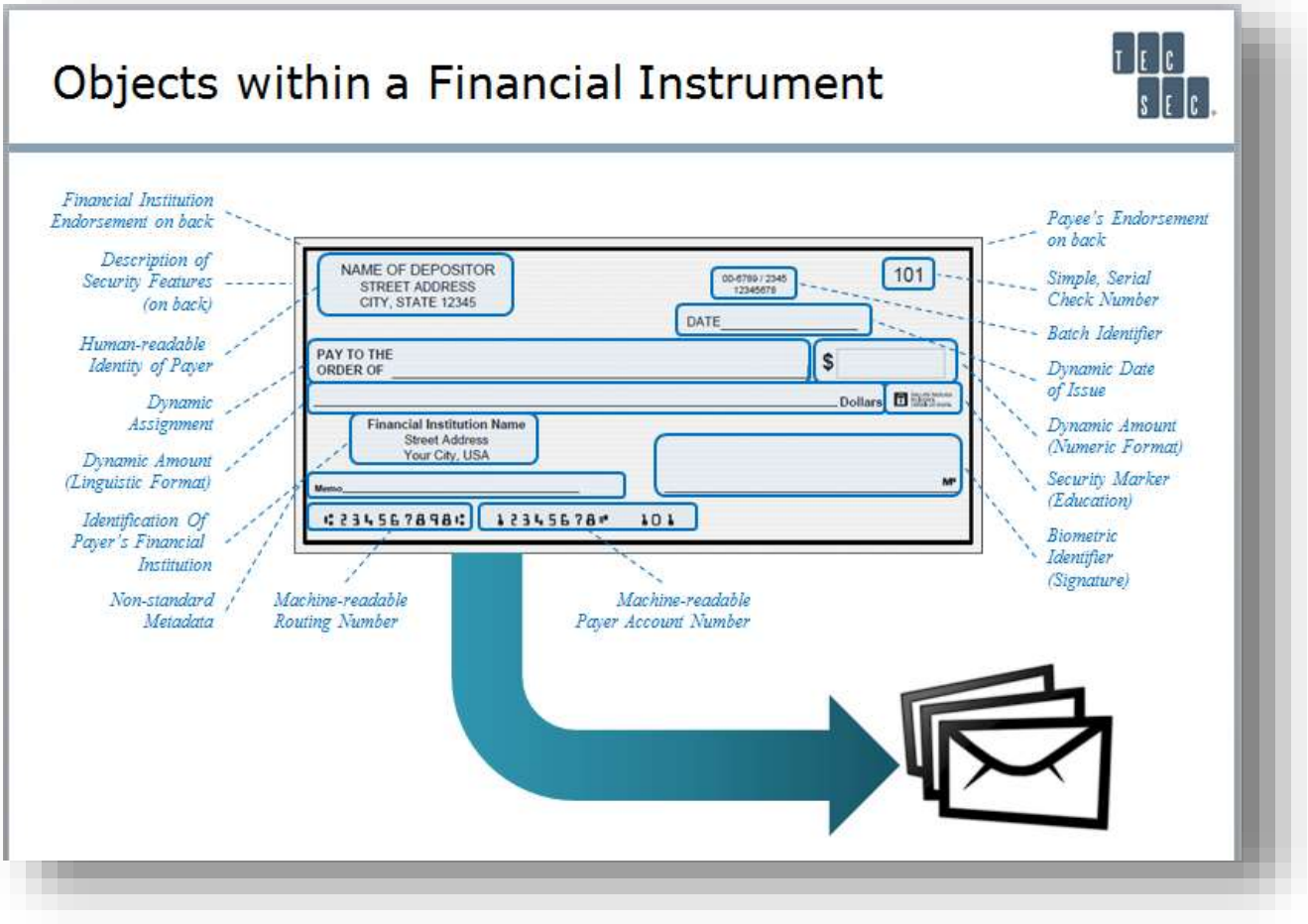

Figure 23 Objects within a Financial Instrument

Objects for Electronic Money

Electronic money, or 'e-money', can take several forms. For example, it can be the money balance recorded electronically on a stored-value card. These cards have microprocessors embedded which can be loaded with a monetary value. Another form of electronic money is network money, meaning software that allows the transfer of value on computer networks, particularly the Internet. Generally, electronic money is a floating claim on a private bank or other financial institution that is not linked to any particular account.[1][1] Or, technology can be used to create "Electronic Money" which is anonymous like cash and not identified to a particular account. Other examples of electronic money are bank deposits, electronic funds transfer, direct deposit, and payment processors. Electronic money can either be centralized, where there is a central point of control over the money supply, or decentralized, where the control over the money supply can come from various sources. Electronic money that is decentralized is also known as digital currencies, or where cryptographic security is used, as

[1] Al-Laham, Al-Tarawneh, Abdallat (2009). "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy".

Copyright 2016
All Rights Reserved

crypto currency. The major difference between e-money and digital/crypto currencies is that e-money doesn't change the value of the fiat currency (USD, EUR) it represents, whereas digital/crypto currency is not necessarily equivalent to any fiat currency, assuming it is not "issued" by a central monetary authority/government (e.g., Bitcoin). In other words, under these definitions all digital currency is electronic money, but electronic money is not necessarily digital currency, unless the digital currency is issued by a central monetary authority/government as "fiat-backed" currency.

Also, many mobile sub-systems have been introduced in the past few years including Google Wallet and Apple Pay. These mobile applications have taken various formats which can be viewed as objects to exercise the payment.

A currency is the value associated with the electronic money application. (Wikipedia 2015)

So, electronic money can be viewed as a potential stepping stone to applying a digital currency once its objects are defined in a standard.

Objects within a Currency

Today's currency takes various forms. In past years, gold was considered a form of currency in the United States with fiat currencies. The following illustration is based on a United States Dollar (USD), but a parallel examination can be done with other country currencies.

In identifying objects for a currency, there are at least two directions to consider: objects which are associated with handling the currency and objects which are associated with the security used in the currency.

Objects for Handling the Currency

To provide identity for the currency, various pictures are included. The USD includes a picture of the US Treasury seal and a Federal Reserve seal as seen in Figure 24.

Detail of the Treasury Seal as it appears on a $1 bill

Example Federal Reserve Bank Seal (for San Francisco) as it appears on a $1 bill

Figure 24 Objects for Handling Currency

Copyright 2016
All Rights Reserved

Other identifying components are included in the dollar representation such as a portrait and other items that would further identify a Dollar from the United States.

The reverse of the one-dollar bill as illustrated in Figure 25 has an ornate design that incorporates both sides of the Great Seal of the United States to the left and right of the word *ONE*. This word appears prominently in the white space at the center of the bill in a capitalized, shadowed, and seriffed typeface. A smaller image of the word "ONE" is superimposed over the numeral "1" in each of the four corners of the bill along with other identifying features.

Figure 25 Identifying Features of the Dollar Bill

The Dollar currency also includes various security objects such as watermarks, color shifting ink, and advanced counter forgery techniques.

Most of these objects can be represented in a digital format. Additional and different types of security objects will be needed to address the risk of a digital forgery.

Objects to Build a Security Schema

Having access to data objects related to a digital currency can offer an efficient means to establish granular levels of confidentiality, data integrity, and security. Some of the physical security techniques used in the Dollar have a minimum countermeasure impact when transformed into a digital environment.

Adding encryption as an enforcement capability at the object level presents a potential countermeasure for environments in which threats will be challenged. Attributes associated with objects can be apparent to selected entities while transparent to the consumer using a digital currency.

Additional examination of these security issues are recommended by the appropriate ISO and ASCX9 committees and work groups to establish a consensus about the role of financial services standards in this area.

Copyright 2016
All Rights Reserved