TECSEC

CKM ENFORCED ENCRYPTION

Providing the Transition From Communication Security to Information Security

Collaboration with business partners is critical to any financial services strategy in executing global commerce. At the same time, effective cooperation with partners within disparate Communities of Interest (COIs) can be effected while preserving participants' privacy and legal rights, sensitive financial data, as well as national and international equities.

An overarching security framework design will facilitate a secure Information Sharing Environment, in a collaborative environment, with mobile remote access or fixed access, based on policy driven requirements. Cryptography can be both an enforcement mechanism as well as a differential access mechanism to enterprise data. Financial environments operate at multiple internal corporate levels, but also need to migrate to different levels of security access under governance, risk and compliance processes that were developed to enable secure sharing and collaboration across multiple cross enterprise information sharing paths.

Secure information flow from multiple sources can be unilateral (tasking), bilateral (fusion), or multilateral (collaborative).   A robust security framework must provide:

- Secure information flow regulated and throttled for the customer in terms of its potential usefulness and value
- Information security integrated into and with existing and available information
- Secure information flow customized in addressing the most pertinent and important problems
- Secure access, but not hindering effective information flow.

The advent of web/internet technologies has shifted the Information Sharing Environment paradigm from static to dynamic; to collaborative over information grids (such as the defined in Clouds); including compute grids, data grids and collaborative grids.

Current links of mobile shared space, to more accessible shared spaces, connected by Corporate and other telecommunications/communications infrastructures like the Internet must be addressed and protected. Credentialized Communities of Interest can gain access to and from other COIs via the Internet with role/attribute based access control (RBAC/ABAC) enforced cryptographically under the control of the data owner organization. Enterprises need to perform real-time analysis on diverse data from disparate data internally as well as externally. This is the integration point where data tagging and labeling contribute by including the appropriate business/policy logics as part of the metadata created by the cryptographic process. The creation of this process of using Persistent tags has been codified in standards published such as International Standards Organization (ISO), American National Standards Institute (ANSI), and NIST standards.

SECURITY FRAMEWORK

JUNE 2014

Metadata environments (e.g., Discovery Metadata Specifications, Emergency Data Exchange Language (EDXL), etc) facilitate real time, live data exchanges, and enable applications for a consistent format to support adjudication of encrypted objects without compromising actual content. Using this approach, different data formats (i.e., structured or flat files, unstructured or multimedia), different infrastructural issues, and different data structures and semantics can be addressed and resolved.

A distributed object oriented environment supports a flexible infrastructure to facilitate information exchange and dynamic discovery. This approach has the following significant advantages:

- Leveraging existing investment in databases, applications, and processes → cost avoidance.
- Existing business rules and processes would be preserved and serve to retain the social fabric → preservation of fiefdoms.
- The information owner could maintain control over the dissemination of information → preservation of equities.
- Privacy safeguards would be in effect → privacy and legal rights.

Another Key Performance Parameter (KPP) is to mechanize an access control process over the information. The data owner would specify the audience/circumstance that has rights to the information and the period of time of access. This approach is highly scalable and supports information flow across the organization(s). Since the information will be disseminated across a variety of systems, the protection must be inherent in the information, preferably done at the object level at rest, in transit or in process.

In addition to protecting the data at the object level and providing protected access to the data, the data can also be protected through a secure tunnel. The secure tunnel offers a different, intermediate point of control at the network layer; whereas, protecting the object offers longer periods of control and time.

Standards and Security Framework

Security has morphed from a point-to-point communication security to a point of presence information security methodology. Object level cryptography with dynamic key management is available for information security. It is necessary to provide the protection process to the data itself as it is not possible to define, in absolute terms, the network; and you cannot defend what you cannot define.

As a proportional response to risk and cost, a federation token can be used as an authentication device, with additional security factors such as biometrics if desired, to bridge a user or machine to the network architecture. An inherent security artifact with information security is that the architecture can be designed such that security can travel with the data while at rest, in transit and in process. Core principles might include:

SECURITY FRAMEWORK

Secure information flow from multiple sources can be unilateral (tasking), bilateral (fusion), or multilateral (collaborative). A robust security framework must provide:

- Secure information flow regulated and throttled for the customer in terms of its potential usefulness and value
- Information security integrated into and with existing and available information
- Secure information flow customized in addressing the most pertinent and important problems
- Secure access, but not hindering effective information flow.

- Information sharing is essential, risk must be mitigated and compliance must be observed.
- The dissemination of information must be based not on organizational principles but rather on a need-to-access basis. Information originally created to serve one can be repurposed for others to affect the Only Handle Information Once (OHIO) principle.
- The process by which individuals access information must be controlled and logged. Safeguards must be used to audit and monitor information access.

Service Oriented Architecture (SOA) and info grids/clouds present a venue to advance the web based service design as the means and the process flow support as well. Major obstacles including platform, operating environment, infrastructure, and database incompatibilities are mitigated using Web Services (WS) to enable a common program-to-program communication, and Extensible Markup Language (XML) to resolve differences in data format. XML serves to standardize data representation into data format such that different applications can read it. Each Enterprise then performs the processing, exploitation, analytics, and production activities in support of related COI activities.

In a SOA environment, the information sharing layer facilitates a person or an application to query. With a standard program-to-program communications interface (i.e., WS), disparate programs can now communicate more easily. The WS model enables programs to be loosely coupled through which a greater flexibility in the services is obtainable. Concurrently, this translates in lower application maintenance costs than those of a tightly coupled process, as well as to enhance interoperability, all while maintaining the confidentiality and controlled access to data objects

XML standardizes data representations such that different applications can read the human and machine readable meta-language enhanced content and data descriptors. This paves the way, first interfacing the human to machine, to be followed by a highly robust machine-to-machine interface, thus accelerating the automation which is critical in the workflow management as well as prevention and reduction of human errors. The object level, dynamic key management approach provides a means to present data, syntax, schema, and semantics for information sharing across multiple enterprises.

The security framework offered here can maximize the use of enterprise restricted data and incorporate distributive access features which have been enforced with encryption. These access features serve to reduce overall cross-domain solution footprint, guard proliferation, and related resource requirements, support data aggregation needed for financial analytics and fusion, improve adaptability of data sources to new dissemination requirements, and improve mandatory access control based on identity and privilege.

Different mathematical models and cryptographic algorithms can be used to provide different assurance models. These different models give rise to different computational constructs to virtualize security domains.

A Standards-based Key Management

A facilitating security technology can be found with cryptography. As an encryption framework, Constructive Key Management (CKM) is designed to facilitate the protection of data, to protect access to data, and to establish a crypto-tunnel.

CKM® is a standards based encryption framework identified in x9 and components of x9, ISO, and NIST standards.

When encrypting with CKM, users or machines label information with Attributes which define the rights required to access the information. Users holding matching Attributes will be able to decrypt the information while those who do not will be unable to view the information.

A unique feature of CKM is that within the CKM process sub-keys are combined to create a data working key for which the all the subkeys are destroyed once the data is encrypted; a symmetric CKM process is later done to reconstruct the working key and to decrypt the information.

An administrative process supports the CKM encryption process. Sub-keys are created, distributed, and stored according to standards established for crypto-key management.

Persistent Protection and More About CKM

Persistent protection with encryption of data itself is a logical next step for firewall network enhancement. Encryption can be viewed in various means and has surfaced as an essential element for protecting information exchanges, for policy enforcement, and for differentiated attribute accesses.

In general, protecting data may be found in traditional secure network tunneling with a Public Key Infrastructure providing the key management support. Protecting the data itself as persistent protection, allows indifference to storage location or network topography. A movement to persistent protection encryption would entail creating self-protecting data objects that are data label aware, with services based on that awareness. The financial services, in the form of an ANSI x9 standard, has published x9.73 which sites a dynamic key management schema called Constructive Key Management® (CKM®).

Persistent Enforcement with CKM® Encryption

Financial Institution Roles

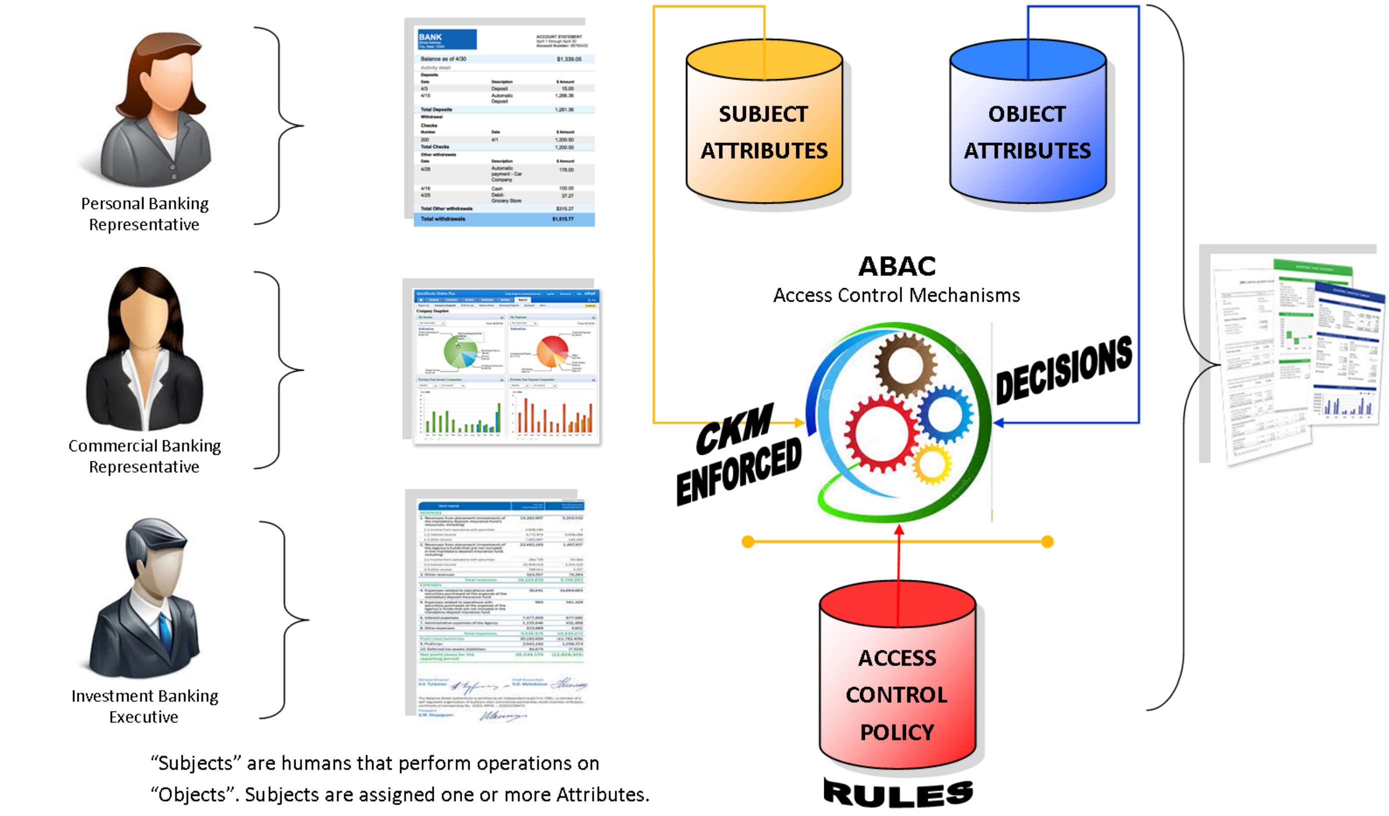
Business transactions are performed by “Subjects” who create and tag “Objects” as part of responsibilities.

Object Attributes

“Objects” tagged with Attributes which define the rights required to access the information.

Access Control

“Objects” can only be accessed by “Subjects” who have the correct set of rights assigned to them.


Personal Banking Representative
Commercial Banking Representative
Investment Banking Executive
SUBJECT ATTRIBUTES
OBJECT ATTRIBUTES
ABAC
Access Control Mechanisms
CKM ENFORCED
DECISIONS
ACCESS CONTROL POLICY
RULES

“Subjects” are humans that perform operations on “Objects”. Subjects are assigned one or more Attributes.

In the above example, staff can tag any file/directory/volume or sub-object which is stored locally or remotely. At rest, the object is encrypted and no care or maintenance is required on the object [it is only encrypted once, though the data may have users at many different access levels]. Only one instance/copy of the object is needed for all supported access levels, rather than multiple instances at each possible access level. In practice, this could be a storage unit in the cloud – if the database or servers were stolen, no specific data destruction policy would need to be completed.

Upon a request for access (authorized or unauthorized) a specific sequence of key descriptors is applied before a key is ever requested. This sequence of key descriptors is basically an “any-to-any” set (multidimensional matrix) of field selectors that are configured a priori. In a traditional model we could describe hierarchical access modes like commercial, regional, executive, investment, stocks.

The key descriptors (attributes) add an important additional functionality, access modes that were heretofore unimaginable at an object level (time of day, branch location, account type, geographic/GPS location, multiple party/shared key, etc) that can be enforced at the time the data object is accessed in any logical method (such as AND, OR). Roles or rules can be applied independently to the attributes associated with each object.

Totally disparate security models may intersect – for example Bank A and Bank B are sharing information but not with Bank C (e.g. posse comitatus). In addition to Attributes, crypto-algorithms such as AES and other international algorithms can limit access to domains while attributes associated with the architecture and schema can further differentiate access.

On a large scale, such as the Clearing House, this level of protection would be available for every object at all times. Data visible to an Executive might show all aspects of a project. When the IT team reviews it, accounting data might be automatically redacted (or vice-versa). HR data might be invisible to the line executive but not to an HR executive.

When implemented as part of a file system, the encryption schema becomes transparent as it is absorbed into an existing, heterogeneous environment. The files can be copied/moved/backed up without concern for whom or how. Identity security can be treated separate from access control. Existing encrypted channels can continue to exist, but with the added encrypted files. Since a single object can serve many views, significant data duplication is eliminated and version control is done from a single document.

In summary, the use of cryptography to enforce policy is available and can be mapped to different computing architectures. Cryptography has expanded beyond only protecting the data channel, but can be directly bound to the data. Leveraging standards based designs offer the financial services market a competitive approach.