



Position Paper - COA Framework

This Collaboration Oriented Architectures (COA) Framework paper describes the requirements for COA-compliant architectures, using an architect's view of the principal components. Where necessary, additional supporting papers describe requirements for specific components.

PRINCIPLES

Relationships and Contracts

- Known parties
- Assurance
- Trust
- Risk
- Compliance
- Legal, Regulatory, Contractual
- Privacy
- Benefits & Obligations

PROCESSES

Collaboration Lifecycle Management

Management processes for:

- People
- Risk
- Information
- Devices
- Enterprises

SERVICES

- Identity Management & Federation & Reputation
- Trust Management & Classification
- Policy Management
- Information Taxonomy & Semantics (Meta-tags)
- Audit

TECHNOLOGIES

Endpoint Security/Assurance

Secure Communications

Secure Protocols

- Wireless
- Mobile Mgt
- VoIP
- Internet Filtering & Reporting

Encryption & Encapsulation

Secure Data

Enterprise Information Protection & Control (Digital Rights Mgt)

ATTRIBUTES OF THE SOLUTION

- Usability/Manageability
- Confidentiality
- Integrity
- Availability
- Efficiency/Performance
- Effectiveness
- Agility

Components of Collaboration Oriented Architectures

The principal components in COA-compliant architectures are grouped into 5 main types:

- Principles
- Processes
- Services
- Attributes
- Technologies

The Principles, and the Attributes of the solution, are described in this paper. The other main types are outlined briefly in this paper, and are further described in appropriate detail in associated COA supporting papers.

1. Principles – Requirements (must haves) and Constraints (shall not).

- *Participating Parties (know who – or what - you're transacting with):*
All components of a transaction chain must be known to the contracting parties at all of its endpoints. These components are selected by collaborating parties, during contract negotiations. Collaborating parties are responsible corporate or individual entities, whose identities are well defined and whose activities are controlled by legal, economic, ethical, and technical means. A collaborating party may be a consortium, in which case the consortium must indemnify its members (and provide other economic, ethical, and technical controls) so that other collaborating parties may safely collaborate with consortium members. In the case where individuals are engaged, they must initiate interaction through an accredited Identity Service Provider.
- *Trust (agree the level of trust/confidence you will be transacting at)*
The collaborating parties have the ability to agree/define appropriate (known) degrees of confidence in the components in a transaction chain, including the environment in which the components are operating.
- *Assurance (verify that the agreed level of confidence pertains)*
Prior agreements between collaborating parties define their obligations to respect each other's intellectual property and to provide adequate technical security during a collaborative transaction.
- *Risk*
The collaborating parties can make an assessment of any proposed transaction based on the communicated levels of trust with factors closely or significantly related to the transaction: identity, confidentiality, integrity, availability, location, environment (space it is being used in), data-sensitivity, transaction value, time, etc.
- *Compliance*
Collaborating parties agree to periodic inspections and security audits. The results of these inspections and audits are published within the collaborative group. Non-compliant parties may be sanctioned or expelled.
- *Legal/Regulatory/Contractual*
The collaborating parties must comply with applicable legal, regulatory, and contractual requirements and be able to resolve conflicts that may arise between these, through effective verification and enforcement mechanisms. Additionally, compliance to local, legal and regulatory requirements alone is unlikely to be good enough to meet all business requirements.

- *Privacy*
Privacy is a particularly important requirement that the collaborating parties must meet. Increasingly, privacy is being defined in legislative safeguards which are the consequence of widespread belief in privacy as a fundamental human right. At its root is an expectation by customers, suppliers, business partners, and employees, that organizations will undertake to use information about an individual ethically so that it is not divulged or otherwise exploited if it is reasonably considered to be "private".
- *Benefits & Obligations*
Contractual obligations, service level agreements, customer expectations, corporate policy, and norms of good corporate citizenship are requirements that need to be aligned and implemented.

2. Processes

See also additional COA supporting papers.

Enterprise processes are evolving as outlined in “[Enterprise 2.0](#)¹” by Professor Andrew McAfee of Harvard Business School, which defined Search, Links, Authorship, Tags, Extensions, and Signals (SLATES) as key transformational elements that are changing the way organisations do business. Well-implemented COA-compliant architectures will maximise the value of collaborations, using various SLATES elements, while managing information risks to an acceptable level.

There are five key Collaboration Lifecycle Management processes (Person lifecycle, Risk lifecycle, Information lifecycle, Device lifecycle, Enterprise relationships – PRIDE) that need to be mastered by organizations that wish to achieve these transformations in a reliable and trustworthy manner.

- *Person Lifecycle Management*
Processes that manage an individual's joining, operational authentication and access management within, and departure from, a collaboration. The processes would also include the management of individuals that are not employees or, more generally, members of the managing entity. Such processes take into account the identity, personas, capabilities, reputation, and potential impact of each of the individuals.
- *Risk Lifecycle Management*
Processes, methods and approaches that identify, classify, and manage the information risks involved in collaborations across organizations.
- *Information Lifecycle Management*
Processes that effectively and efficiently manage the creation, reading, update and deletion of information assets in a collaboration. These processes would include audit, monitoring and information protection activities.
- *Device Lifecycle Management*
Processes for introducing devices, identifying and maintaining device trust levels, and removing devices involved in collaborations. Removal of devices involves eradication of all information assets from the device.
- *Enterprise Relationship Management*
Processes that ensure that collaborations are managed according to the state of the relationships involved and the value and/or risks they introduce. Initiating, operating, and closing down collaborations emanating from an enterprise would include a means of

¹ Dion Hinchcliffe, Oct 22nd 2007: “The State of Enterprise 2.0” - <http://blogs.zdnet.com/Hinchcliffe/?p=143>

mapping the critical relationships between all the collaborating parties. Such processes would also have the ability to identify collaborating parties that are endangering the enterprise, and rapidly close down offending relationships. The processes would also have the ability of identifying the most valuable relationships in order to ensure their appropriate development and protection. Such processes are also valuable during, mergers, acquisitions or divestitures.

3. Services

See also additional COA supporting papers.

These services may be provided by one or more of the collaborating parties, or a 3rd party. Whichever one is used will have significant ramifications on how the services are provided.

- *Identity Management, Federation, and Reputation*
The credentials of principals (organizations, individuals, systems, devices), and associated attributes required for identification, authentication and authorization decisions, should be expressed in a standardised form, so they can be validated and accepted by the systems of any member of the collaboration or service providers.
- *Policy Management*
The collaborating parties, and service providers, have the ability jointly or separately to evaluate, manage, and implement the policies and rules for authorizing and de-authorizing principals and collaborating parties.
- *Trust Management*
 - *Business Impact Levels*
A common language and set of definitions for Business Impact Levels is required. We propose defining 5 levels:
 - Catastrophic
 - Material
 - Major
 - Minor
 - Insignificant

NB: Financial levels would be different for different individuals and enterprises.
 - *Information Classification*
A common taxonomy is required for defining the sensitivity of Information Assets aligned with risk-based assessment of business impact of an incident or threat. There are identity, legality and temporal components of information classification, all of these being context-sensitive. We propose basing information sensitivity on the G8 Traffic Light Protocol – 4 levels:
 - White - public
 - Green – identified business community
 - Amber – established named groups only
 - Red – specific to named recipients only
 - *Impact Sensitivity Categorization*
The requirement here is to develop a common language (taxonomy) and set of trust levels defining impact sensitivity of information, based on measures of it's Confidentiality, Integrity, Authenticity, & Availability. (Note that Service or System Criticality is potentially a separate area of classification.)

We propose 6 levels:

- T5 Catastrophic
- T4 Material
- T3 Major
- T2 Minor
- T1 Insignificant
- T0 None

○ *Control Stratification*

A set of standardised Information Trust Categories by Trust Level is required, using the standard CIA frame and adding identity. An example outline of what might be an acceptable solution would be to define a 6-level trust taxonomy for authenticity as:

- C5 ASSURED (biometric)
- C4 AFFIRMED (positive physical or logical authentication)
- C3 PROVEN (authenticated by trusted third entity)
- C2 CONFIRMED (confirmed by strong attributes)
- C1 ASSERTED (self-asserted)
- C0 UNKNOWN (no authenticity assertions made - anonymous)

○ *Architecture Segmentation Model*

A coherent architectural model is required to map the Trust Management components (business impact levels, information sensitivity levels, information sensitivity levels, and Confidentiality, Integrity, Availability, Identity category levels) into an effective operationally aligned structure.

● *Information Taxonomy and Semantics*

This has also been described as Meta-Information Asset Management. This component addresses the requirement for collaboratively-shared data to be appropriately secured in storage, transit, and use - based on the agreed risk and performance requirements for the information contained in this data as a result of its Classification. Principals accessing the data are identified, authenticated, and authorized. These requirements must be maintained through the complete document lifecycle, from creation through to destruction, by an appropriate Information Lifecycle Management process (see Processes, section 2).

● *Audit*

Transfers, storage, and retrievals of collaboratively shared data, and associated business controls, are auditable events. There is an associated requirement for a common notion of 'event' across all collaborating parties and systems. Collaborating parties may require each other to conduct spot-audits on individual data objects and the actions associated with them, either overtly or without alerting the individuals using these objects to the increased audit activity. The collaborative group may require summary audit reports on data transfers, storage, and retrievals to be published at some regular interval within the group. The audit information needs to be of adequate quality to meet the needs of each collaborating organization, including the rigor required for forensic evidence in law. A key driving principle in audits on COA-compliant architectures is transparency between partners.

4. Attributes

Attributes enable you to measure whether you are achieving your objectives.

- *Usability/Manageability*
Security measures are non-intrusive, are readily managed by the relevant governing enterprises, and are easily understood by the individual end user.
- *Availability*
Information shared between collaborating organizations should not be rendered unavailable either by mistake or by an adversary. This implies that any ‘at rest’ encryption keys are escrowed, and that information is held in open-standard formats.
- *Efficiency/Performance*
Security measures should not greatly affect the latency, bandwidth, or total cost of data retrieval, storage, or transmission. This implies that collaborating partners must possess the means to rapidly access decryption keys for all data in their possession for which they continue to have access privileges, allowing rapid data retrievals and offline malware scans.
- *Effectiveness*
COA-compliant architectures should provide an effective approach to organizing and controlling secure data transport and storage among a wide range of existing and future corporate information systems.
- *Agility*
COA-compliant architectures must take into account the dimensions of timeliness and flexibility, so as to enable development of business-driven enterprise architectures that are appropriately flexible and adaptable to facilitate changes in business operations with optimal rapidity and ease, with minimal disruption.

5. Technologies

See also additional COA supporting papers.

Key technologies required to deliver Services (see section 3) include:

- Endpoint Security/Assurance
 - Secure Communications
 - Secure Protocols (Wireless, Mobile Mgt, VoIP, Internet Filtering & Reporting)
 - Encryption & Encapsulation
 - Secure Data
 - Enterprise Information Protection & Control (Digital Rights Management in the enterprise, rather than the performing arts industry)
-