CSAP

COMMON SECURITY ARCHITECTURE
for PRODUCTION

VERSION 1.2

PART 3:
SECURITY LEVELS

Contents

This document is intended as a guide for companies developing or implementing products, solutions, or services for the future of media creation. No effort is made by Motion Picture Laboratories, Inc. to

obligate any market participant to adhere to the recommendations in this document. Whether to adopt these recommendations in whole or in part is left to the discretion of individual market participants, using independent business judgment. Each MovieLabs member company shall decide independently the extent to which it will utilize, or require adherence to, these recommendations. All questions on member company adoption or implementation must be directed independently to each member company.

1 Introduction

This document is Part 3 of the security architecture documents. Familiarity with "Part 1: Architecture Description" is necessary to understand this document; however, it is not necessary to have reviewed "Part 2: Interfaces" before reading this document.

This document looks at how security can be scaled in an orderly manner. The primary driver for scalable security is that higher levels of security tend to cost more. If that were not the case, the maximum level of security likely would be employed universally.

This security architecture enables the security to be scaled to accommodate a production's risk tolerance, and this document is an illustration of how that scaling might occur in practice.

Changes from CSAP Part 1 v1.1

- The name of the *authorization policies* has been changed to *authorization rules*.
- The functions of the policy manager moved into the authorization service, the policy service in v1.0 now consists only of the Authorization Rules Distribution Service (ARDS), formerly called the ARDS. This does not change the functions necessary to create an authorization policy, but consolidation simplifies this part of the architecture.

1.1 Abbreviations

ARDS **-** Authorization rules distribution service.

PEP **-** Policy enforcement point.

1.2 Risk

Risk assessment is a combination of the likelihood of an event happening and the consequences of it doing so. When combined with the cost of mitigation, we get an expression of risk tolerance. Understanding risk tolerance allows decisions to be made about which risks to mitigate and to what extent. However well the security is designed and implemented, greater security is typically more expensive in terms of operating expense (OpEx), as well as capital expenditure (CapEx) if the implementation is not entirely in the cloud. Whether formal or informal, the outcome of a risk management[1] process is a guide to how robust the security needs to be – the scaling of security.

The required level of security may vary for one production. For example:

- A motion picture may have different security requirements for editors creating sequences with synchronized sound than for an in-house effects group working on an air-gapped network.
- A TV series may have tighter security requirements for the season opener and the season finale than for the episodes in between.

[1] There are many accepted methods of assessing risk, such as ISO 31000:2018,[1] Risk Management Guidelines https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

1.3 Security Levels

In order to illustrate scalability, we need some sort of measure, and this document uses the construct of security levels to present a quantitative rather than qualitative view of scalability.

We will use three levels:

Security Level	Description	Example application
100	The minimum level of functionality and capability	The majority of productions where CSAP can provide better security management
200	The robust level of functionality and capability	A scripted TV series increases security in editorial and finishing to level 200 for its season finale
300	The highest level of security	A major motion picture uses level 300 for sensitive assets

The use of 100, 200 and 300 is arbitrary. We could equally have used low, medium and high.

The presence of a component is shown for each level using the classifications *beneficial* and *necessary*.

A particular security system meets, for example, level 200, if every component meets the criteria for level 200 or better.

A component that interacts with another component may function when the second component is not available, although perhaps at a reduced level of security. Best practices say that if two components are available in an implementation and are defined in the full architecture with one making use of the other, the one should make use of the other.

Capability may be expressed as localized and system-wide capability.

Capability Category	Explanation
Localized	The capability is present in one or more parts of the system
System-wide	The capability is present throughout the system in an integrated manner.

Note that a requirement to support a feature is not a requirement to use the feature.

1.4 Use

There are two observations about CSAP security levels that are important:

- Not every service or technology needs to be capable of level 200 or 300 – the security level is determined by production security requirements
- Workflows within a single production may use different CSAP levels

CSAP security levels can be chosen for a variety of reasons. The decision as to which security level to use for any part of a production is based on an assessment of the risk and the cost.

Risk assessment, whether formal or informal, looks at the likelihood of a security event occurring and any detrimental outcome. Cost means the cost, in the broadest sense, of mitigating risk.

1.5 Categorization of Authorization Policies

Authorization policies can be created during the initialization phase of a workflow or when a task is scheduled. They may be valid for a period that is, for example, the duration of the production, the duration of a workflow (e.g., an authorization policy is valid while dailies are being produced) or the duration of a task.

This affects the implementation of CSAP authorization policies. For that reason, and for the purposes of this document, we introduce the following imprecise[2] categorization of authorization policies.

Authorization Policy Category	Explanation
Short lifetime	Authorization policies are created for each task and the lifetime is approximately the duration of the task
Medium lifetime	Authorization policies are created for each workflow and the lifetime is approximately the duration of the workflow
Long lifetime	Authorization policies are created for each workflow and the lifetime is the duration of the production or a phase (e.g., post-production) of the production

Please note that CSAP Part 1 version 1.2 removed the distinction between static and dynamic security policies, since they behave the same and the difference was in implementation, and are now simply "*authorization policies.*"

There are no functional differences between the authorization policies in each category, the difference is in the lifetime. This is important to this document because it describes what level of capability for authorization policies is necessary.

1.6 Functionality vs. Components

CSAP security levels are defined by functionality and components. The functions necessary in a level determine the components that are necessary.

1.7 CSAP and Workflow Automation

CSAP is workflow driven security designed to be responsive to workflow automation with a great deal of granularity. Workflow automation isn't a CSAP requirement, it works however workflow management operates.

In Part 4: Securing Software-Defined Workflows, we discuss workflow management and break it down into two phases:

- Initialize. For example:

[2] There isn't a hard boundary between each category.

    - A production department is established, the crew hired, and resources acquired
    - The necessary security level is defined
    - The crew agree on a workflow between themselves and with other departments
- Execute. For example, a dailies department workflow:
    - Wait for data to arrive from set
    - Sync sound, edit footage, color grade footage
    - Director reviews and decides what to distribute
    - Dailies are sent to dailies distribution and editorial
    - Repeat…

Both phases are likely to be a combination of manual and automated work. In initialization, on-boarding might be an automated process but the crew agreeing on a workflow is probably manual. In our example of execution, it likely a goal that data movement and scheduling are automated but a task like color grading will be part automation and part manual.

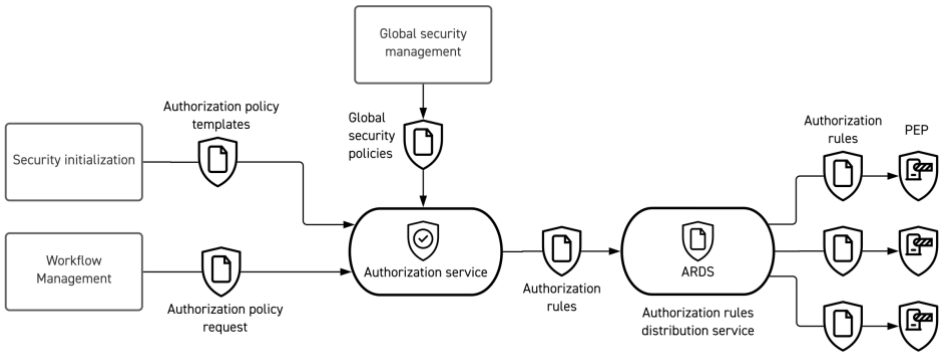

Figure 1-1 Authorization policy creation

If we look at authorization policy creation, see figure above, the initialize phase generates the authorization policy templates and can generate requests for authorization policies. The execute phase is primarily interested in requesting the creation of authorization policies. However, whether the phases are automated or not does not change how CSAP operates.

1.8 Scope of CSAP Part 3

CSAP is a collaboration-oriented zero-trust security architecture. It is concerned with securing and protecting the integrity of assets, processes, and workflows in the collaborative environment of media production. The scope of this document is the CSAP functions required to reach certain defined levels of operation. The higher the CSAP security level, the higher the level of security possible.

CSAP is not a set of recommended practices for security or set of security controls. Every artifact that is trusted is assumed to have a sufficient level of protection implemented to ensure that it is trustworthy but the standard by which that is judged is outside of the architecture. CSAP and its Policy Enforcement Points are there to ensure that only authenticated and authorized activity, for example network connections, takes place.

It is not the role of CSAP to ensure that a trusted artifact is indeed trustworthy. How that is achieved, and the level of robustness, are matters for implementation based on, for example, organization requirements and risk analysis.

However, common sense says that authorization should not extend beyond the bounds of how trustworthy something is. Furthermore, authentication does not have to be binary (authenticated or not authenticated). CSAP has the concept of a trust score. Services such as trust inference can be used to modulate to how much something is trusted – for example, a user that might otherwise be authorized to access the most sensitive assets might be limited to less sensitive assets if their trust score isn't 100% because they logged in from a new location.

2 Security Levels for Core Security Components

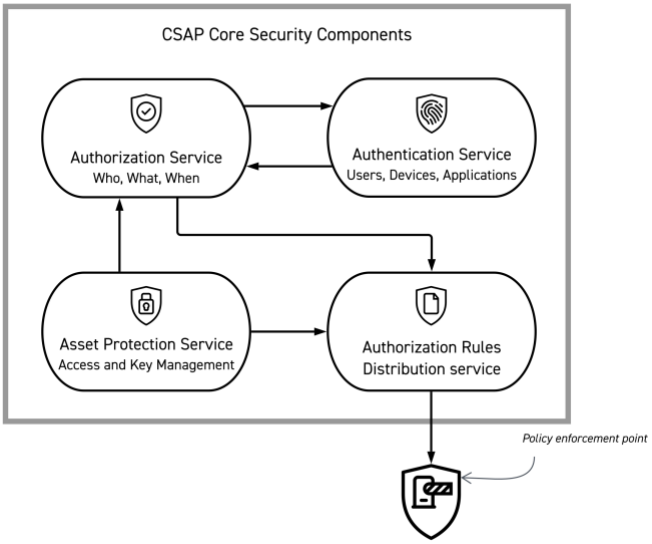

Figure 2-1 Core security components

The rest of this section details the requirements for the presence of the components.

2.1 Authentication Service[3]

Level	Presence
100	• Authentication service necessary
200	• Authentication service necessary
300	• Authentication service necessary

[3] Each level is required to support the entity authentications required for that level, as described below

2.2 Authorization Service[4]

Level	Presence
100	• System-wide capability for long lifetime authorization policies necessary • Localized capability for medium and short lifetime authorization policy beneficial
200	• System wide capability for long lifetime authorization policies necessary • Localized capability for medium lifetime authorization policies necessary • Localized capability for short lifetime authorization policy beneficial
300	• System wide capability for medium lifetime authorization policies necessary • Localized capability for short lifetime authorization policies necessary

2.3 Asset Protection Service

Level	Presence
100	• Protection by access controls necessary • Asset encryption capability beneficial
200	• Protection by access permissions necessary • Local asset encryption capability necessary • End-to-end asset encryption capability beneficial
300	• End-to-end asset encryption capability necessary

In CSAP Part 1, we categorize encryption of stored assets we define two classes:

- **Implicit encryption**. We define implicit encryption to mean that whatever is holding the asset (a storage "container,"[5] such as a disk, or a filesystem volume) is encrypted. Typically, the encryption is a property of the infrastructure; the container is encrypted as a property of the storage mechanism.
- **Explicit encryption.** We define explicit encryption to mean assets are encrypted individually or as a group such that the encryption is independent of how the assets are held. We refer to this as "asset encryption." It is also referred to as "file encryption."

Since implicit encryption is widely used and supported by most storage systems, we regard it as a property of the infrastructure and do not call it out in the CSAP levels. The use of implicit encryption is a matter for security assessments.

[4] Each level is required to support the Authorization Policies required for that level, as described below.

[5] Including object storage, file storage, block storage, volume storage, hard drives…

The capability for explicit asset encryption requires additional capabilities in the infrastructure.

End-to-end asset encryption means that an asset is encrypted at or close to the point of creation and is decrypted at, or close to, the point of consumption. Local asset encryption means that it is encrypted throughout its lifecycle but may be decrypted and re-encrypted along the way (with appropriate key rotation).

Explicit asset encryption can be extremely discriminatory, and key management and decryption are outside of the storage system.

2.4 Authorization Rule Distribution Service (ARDS)

Level	Presence
100	ARDS necessary
200	ARDS necessary
300	ARDS necessary

3 Security Levels for Supporting Security Components

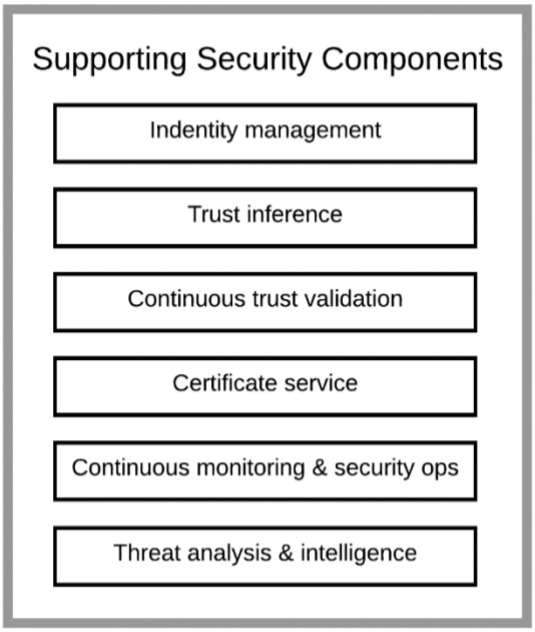

Figure 3-1 Supporting security components

3.1 Identity Management

Security Level	Presence
100	• Identity management necessary
200	• Identity management necessary
300	• Identity management necessary

3.2 Trust Inference

Security Level	Presence
100	• Trust inference beneficial
200	• Trust inference beneficial
300	• Trust inference necessary

3.3 Continuous Trust Validation

Security Level	Presence
100	• Continuous trust evaluation beneficial
200	• Continuous trust evaluation beneficial
300	• Continuous trust evaluation necessary

3.4 Certificate Service

Security Level	Presence
100	• Certificate service necessary
200	• Certificate service necessary
300	• Certificate service necessary

The certificate service might be implemented as a public or private certificate authority.

3.5 Continuous Monitoring and Security Operations

Security Level	Presence
100	• CMSO beneficial
200	• CMSO beneficial
300	• CSMO necessary

Continuous monitoring and security operations (CMSO) is a set of functions conducting real-time analysis of multiple data sources to provide situational awareness to other security components and to the information security operations center (ISOC).

3.6 Threat Analysis and Intelligence

Security Level	Presence
100	• Threat analysis and intelligence beneficial
200	• Threat analysis and intelligence beneficial
300	• Threat analysis and intelligence necessary

4 Aggregated Security Levels

This section shows the beneficial and necessary components by security level.

4.1 Level 100

Necessary Core Components	Beneficial Core Components

• Authentication service
• Authorization service
  ○ System wide capability for long lifetime authorization policies
• Asset protection
  ○ Access controls
• ARDS
	• Authorization service
	  ○ Localized capability for medium and short lifetime authorization policies
	• Asset protection
	  ○ Local asset encryption capability
	  ○ End-to-end asset encryption capability

Necessary Supporting Components	Beneficial Supporting Components
• Identity management • Certificate service	• Trust inference • Continuous trust evaluation • Continuous monitoring and security operations (CMSO) • Threat analysis and intelligence

4.2 Level 200

Necessary Core Components	Beneficial Core Components

• Authentication service
• Authorization service
  ○ System wide capability for long lifetime authorization policies
  ○ Localized capability for medium lifetime authorization policies
• Asset protection
  ○ Access controls
  ○ Local asset encryption capability
• ARDS
	• Authorization service
	  ○ Localized capability for short lifetime authorization policies
	• Asset protection
	  ○ End-to-end asset encryption capability

Necessary Supporting Components	Beneficial Supporting Components
• Identity management • Certificate service	• Trust inference • Continuous trust evaluation • Continuous monitoring and security operations (CMSO) CMSO • Threat analysis and intelligence

4.3 Level 300

Necessary Core Security Components	Beneficial Core Security Components

• Authentication service
• Authorization service
  ○ System wide capability for long lifetime authorization policies
  ○ System wide capability for medium lifetime authorization policies
  ○ Localized capability for short lifetime authorization policies
• Asset protection
  ○ Access controls
  ○ Local asset encryption capability
  ○ End-to-end asset encryption capability
• ARDS	

Necessary Supporting Security Components	Beneficial Supporting Security Components
• Identity management • Trust inference • Continuous trust evaluation • Certificate service • Continuous monitoring and security operations (CMSO) • Threat analysis and intelligence	

5 Intra-Component Automation

Intra-component automation means automation between each of the core and supporting security components.

CSAP is built on the assumption that during the execute phase of a workflow, certain intra-component interactions can be, but are not required to be, automated.

Although it is a highly desirable in implementing an efficient and responsive system, automation is not a requirement for CSAP. For that reason,[6] we do not include automation in the requirements for each security level.

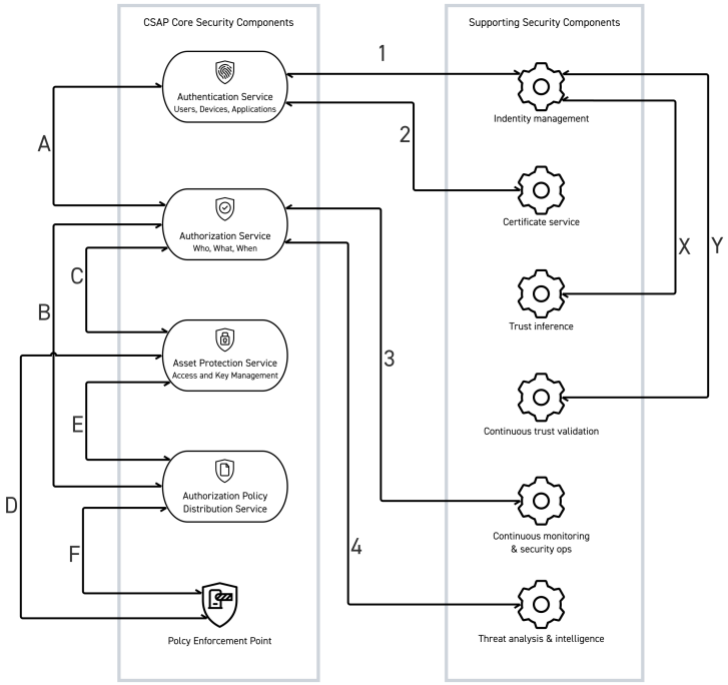

Figure 5-1 Primary intra-component interfaces

Automation is recommended for intra-component interactions where operation is either time critical or a missing interaction can cause a security issue. (We are assuming that an automated process is less likely to "overlook" something).

Using the interfaces as annotated in the figure above, we create our list:

Reference	Description	Level 100	Level 200	Level 300
A	Authentication/Authorization		Recommended	Recommended
B	Authorization/ARDS	Recommended	Recommended	Recommended
C	Authorization/Asset protection		Recommended	Recommended

[6] And because the desire and ability to implement automation starts with the workflow.

Reference	Description	Level 100	Level 200	Level 300
D	Asset protection/PEP*		See note	See note
E	Asset protection/ARDS		See note	See note
F	ARDS/PEP	Recommended	Recommended	Recommended

Note: The need for automation of the interfaces associated with asset protection depends on how asset protection is achieved and to what granularity. Asset level encryption is a strong candidate for automation, whereas access control through ACLs may not be.

Reference		Level 100	Level 200	Level 300
1	Authentication/Identity management		Recommended	Recommended
2	Authentication/Certificate service		Recommended	Recommended
3	Authorization/Continuous monitoring & security operations			Recommended
4	Authorization/Threat analysis & intelligence			Recommended

Reference		Level 100	Level 200	Level 300
X	Identity management/Trust inference			Recommended
Y	Identity management/Continuous trust validation			Recommended