MOVIELABS
SECURITY ARCHITECTURE
PART 3:
SECURITY LEVELS
VERSION 1.0

Contents

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.

1.1 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.

1.2 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.

This construct is neither an expression of requirements nor a proposal.

[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.

We will use three levels:

Security Level	Description	Example application
100	The minimum level of functionality and capability	An unscripted production with a high level of risk tolerance
200	The robust level of functionality and capability	A scripted TV series with a medium level of risk tolerance
300	The highest level of security	A major motion picture with near-zero risk tolerance

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.

2 Security Levels for Supporting Security Components

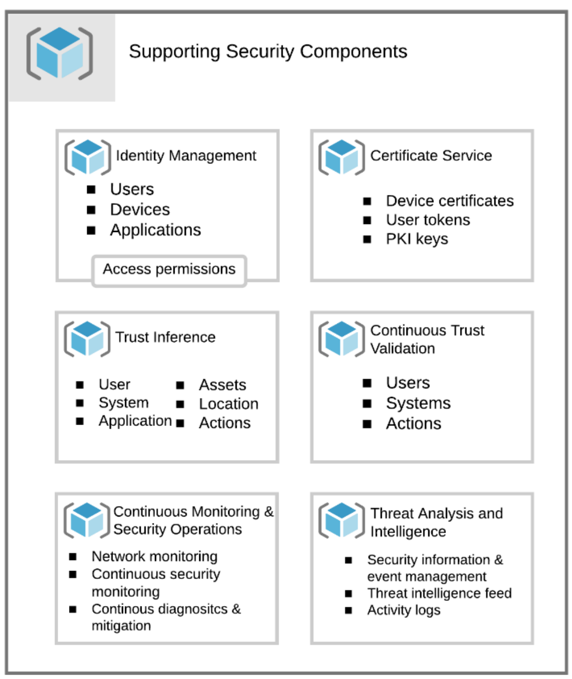

Figure 2-1 Detailed view of supporting components

2.1 Identity Management

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

2.2 Trust Inference

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

2.3 Continuous Trust Validation

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

2.4 Certificate Service

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

2.5 Continuous Monitoring and Security Operations

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

2.6 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

3 Security Levels for Core Security Components

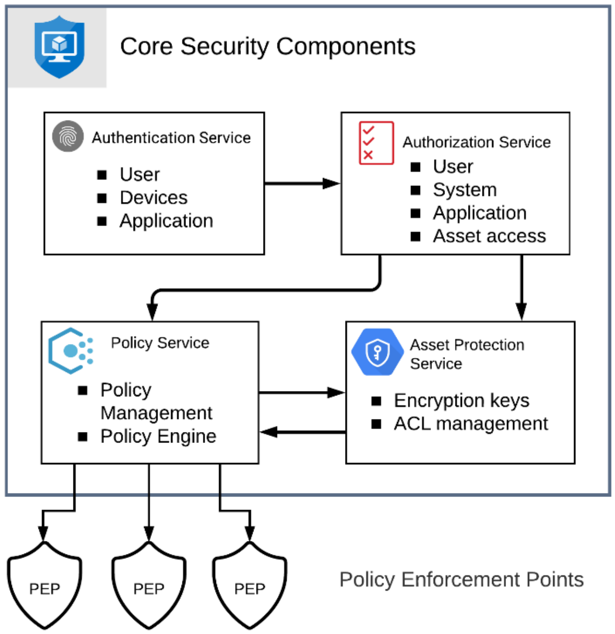

Figure 3-1 Detail of core components

3.1 Authentication Service

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

3.2 Authorization Service

Level	**Presence**
100	• Authorization support for Static Policies
200	• Authorization support of Broad Dynamic Policies
300	• Authorization support of Specific Dynamic Policies

3.3 Asset Protection Service

Level	Presence
100	• Static Policy access controls necessary • Dynamic access controls beneficial
200	• Dynamic Policy access controls necessary • Asset encryption beneficial
300	• Asset encryption necessary

3.4 Policy Service

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

4 Aggregated Security Levels

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

4.1 Level 100

Necessary Components

- Identity management
- Certificate service
- Authentication service
- Static access controls
- Policy service

Beneficial Components

- Trust inference
- Continuous trust evaluation
- Dynamic access controls
- CMSO
- Threat analysis and intelligence

4.2 Level 200

Necessary Components

- Identity management
- Certificate service
- Authentication service
- Dynamic access controls
- Policy service

Beneficial Components

- Trust inference
- Continuous trust evaluation
- CMSO
- Threat analysis and intelligence
- Asset encryption

4.3 Level 300

Necessary Components

- Identity management
- Trust inference
- Continuous trust evaluation
- Certificate service
- CSMO
- Threat analysis and intelligence
- Authentication service
- Authorization support of specific dynamic policies
- Asset encryption
- Policy service