A Security Solution for Information Service in SWIM

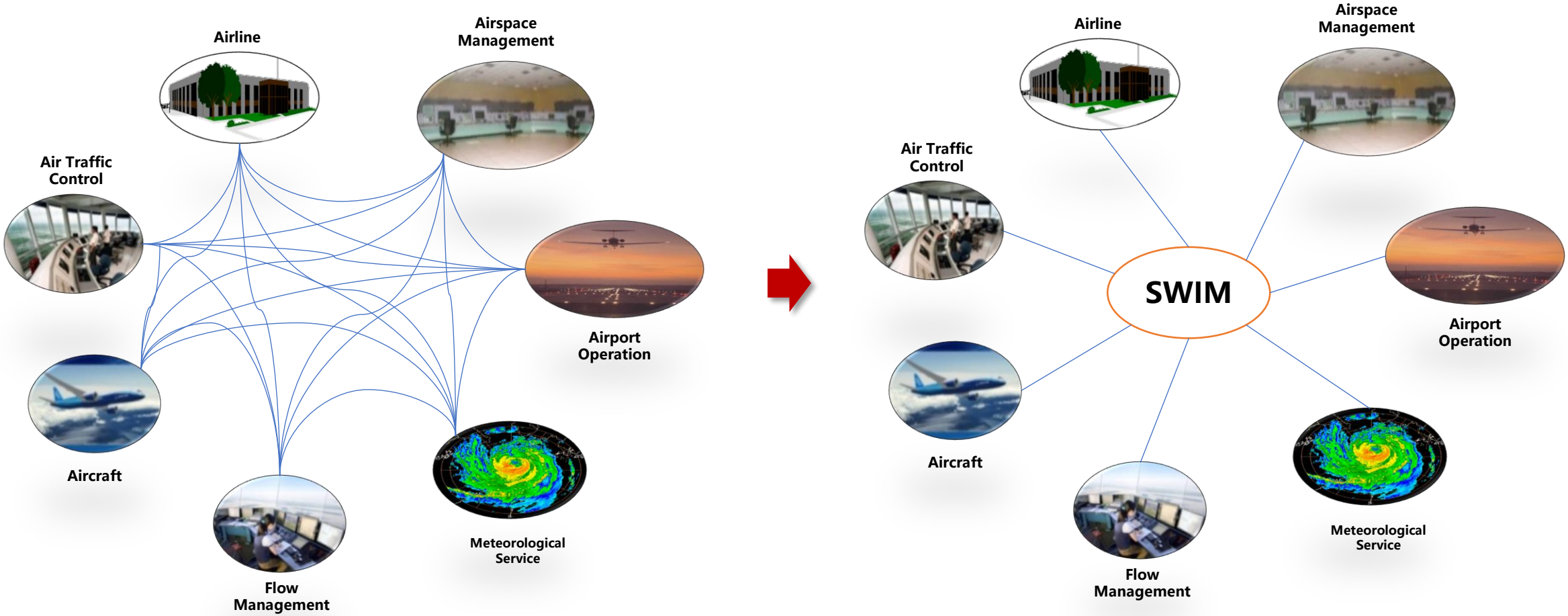
Tian Yungang
June 2021

State Key Laboratory of Air Traffic Management System and Technology, China

Contents

1. Introduction

Transformation of ATM System

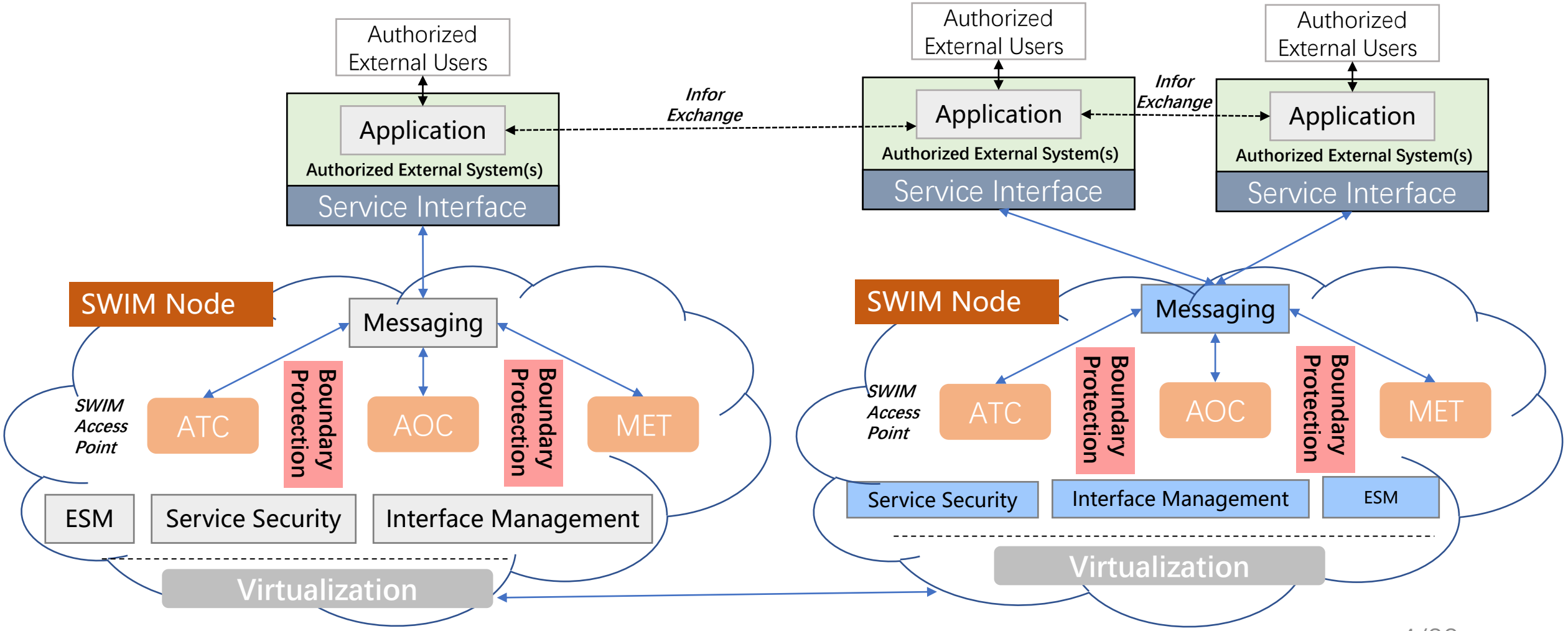


Current ATM system

SWIM enabled ATM system

1. Introduction

Transformation of ATM System



1. Introduction

Security Threats:

Unauthorized access: access to data without prior consent, resulting in information leakage;

Tampering: **u**nauthorized changes to data (changing security control settings or modifying flight data)

Spoofing: conduct cyber attacks by impersonating the identities of legitimate users

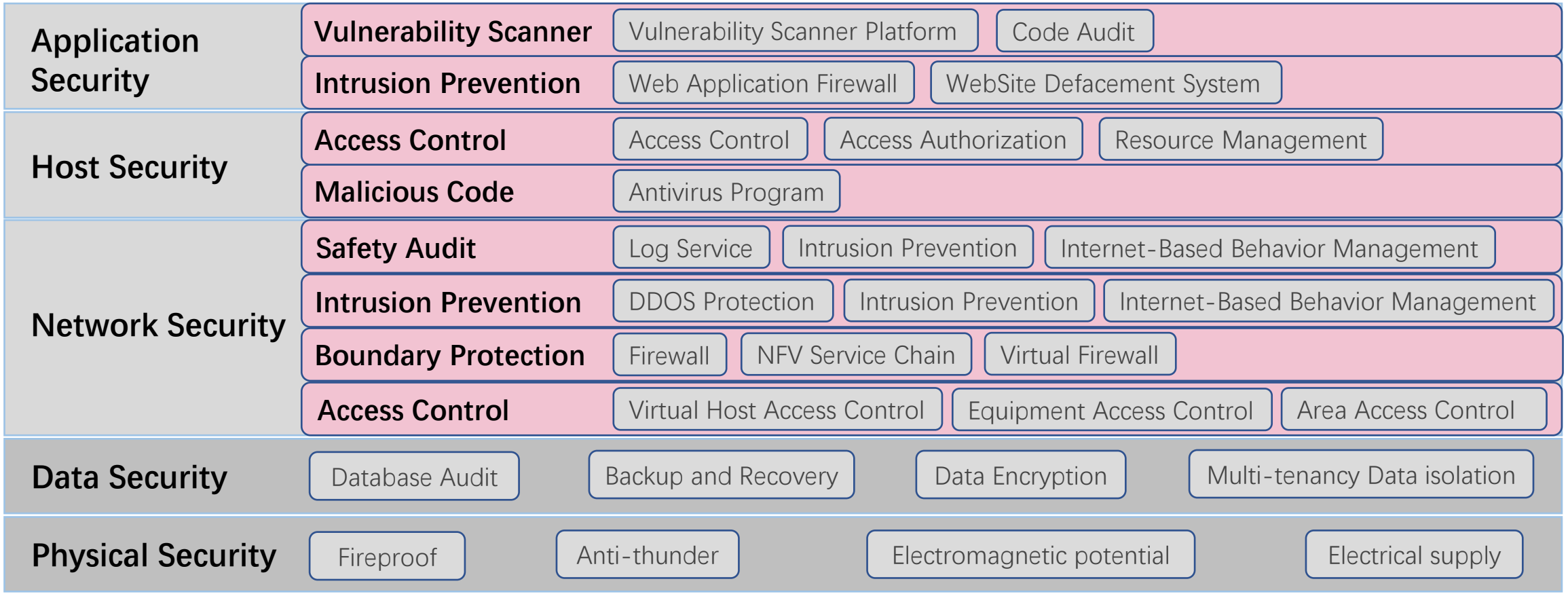
Deny access: prevent legitimate users from accessing information

Computer virus: spread computer viruses through the network, causing information leakage or system unavailability

Multi-tenant: problem of breaking through the virtual logic isolation to obtain other virtual machine information or reduce its performance (commonly used side-channel attacks)

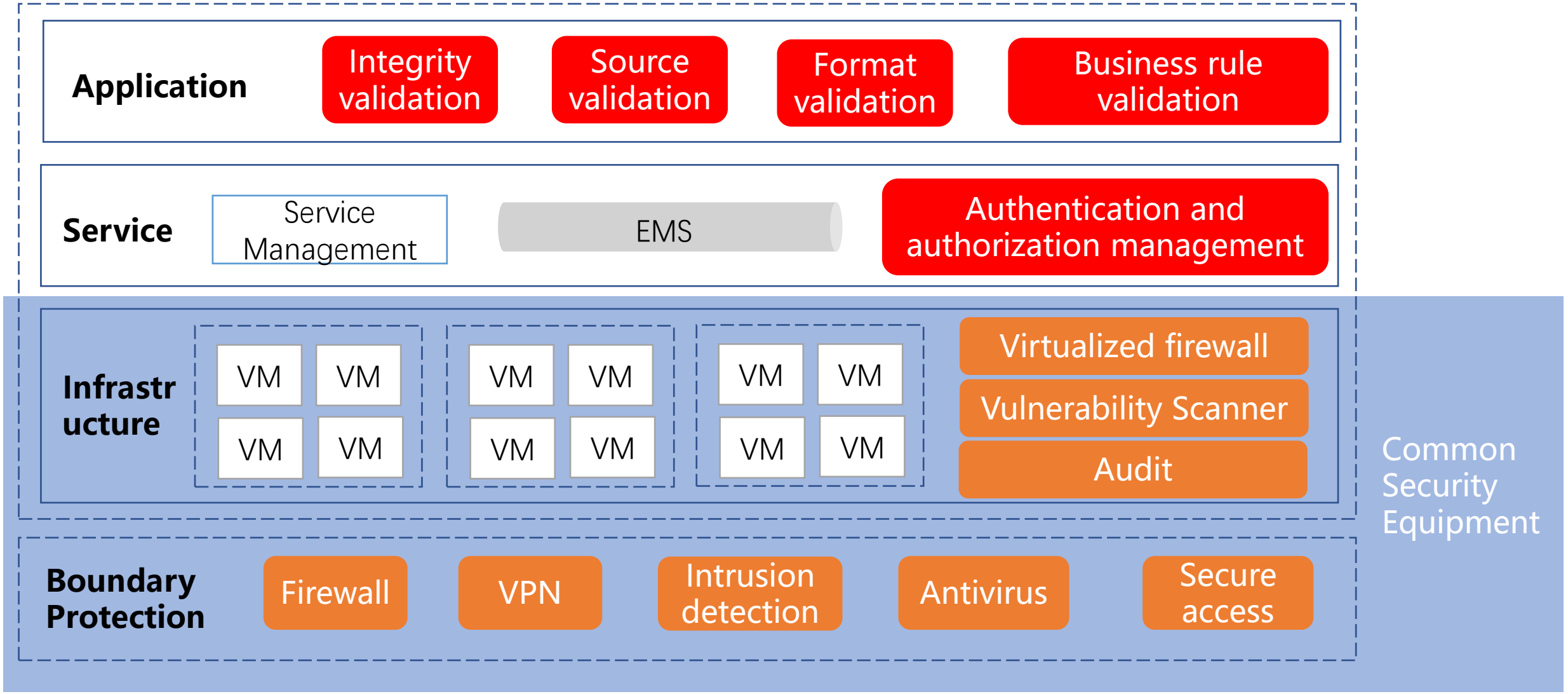
1. Introduction

Security Requirements



Contents

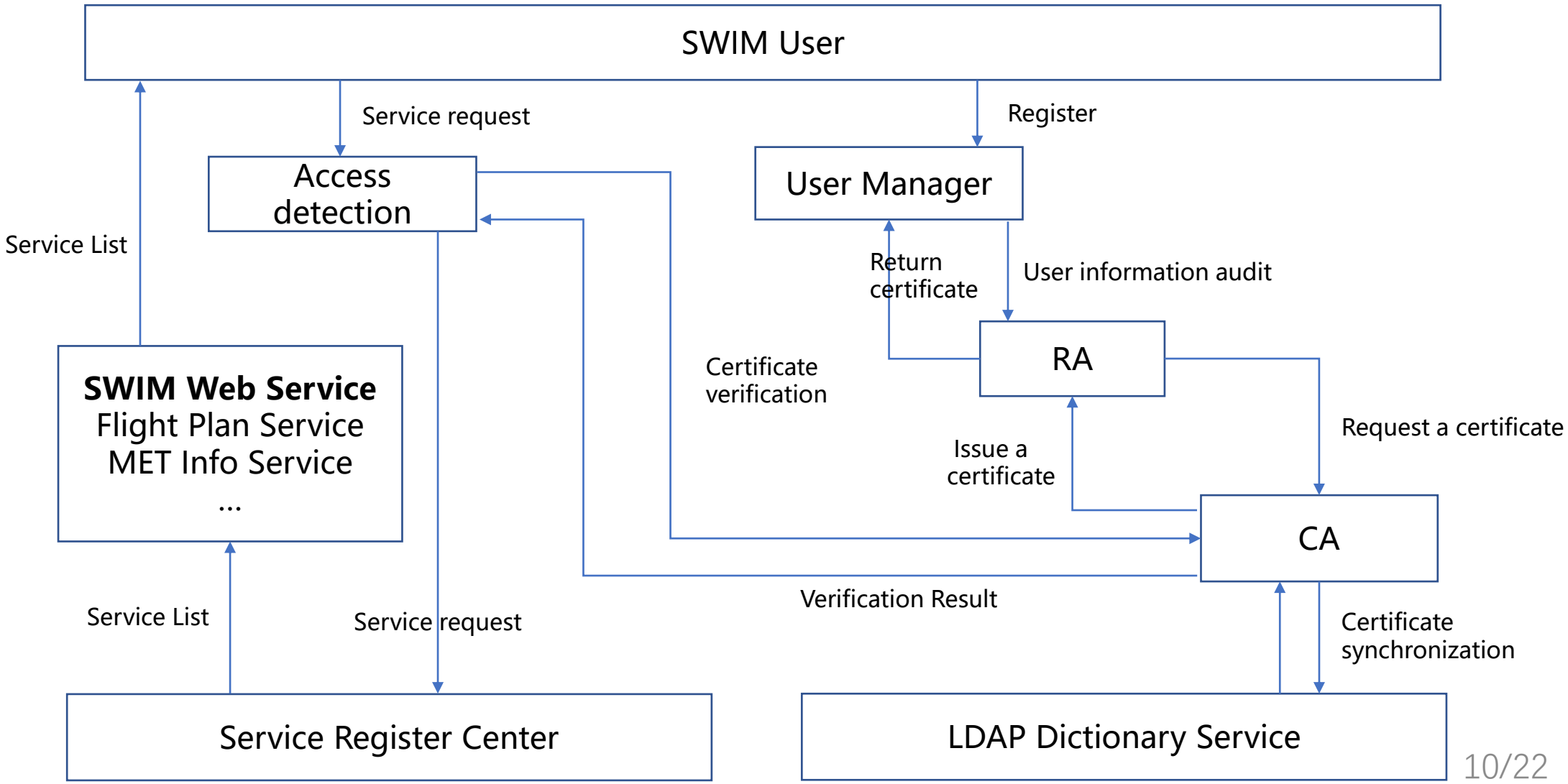
2. Framework


Application
Integrity validation
Source validation
Format validation
Business rule validation
Service
Service Management
EMS
Authentication and authorization management
Infrastr ucture
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
Virtualized firewall
Vulnerability Scanner
Audit
Common Security Equipment
Boundary Protection
Firewall
VPN
Intrusion detection
Antivirus
Secure access

Contents

3. Solutions

Authentication



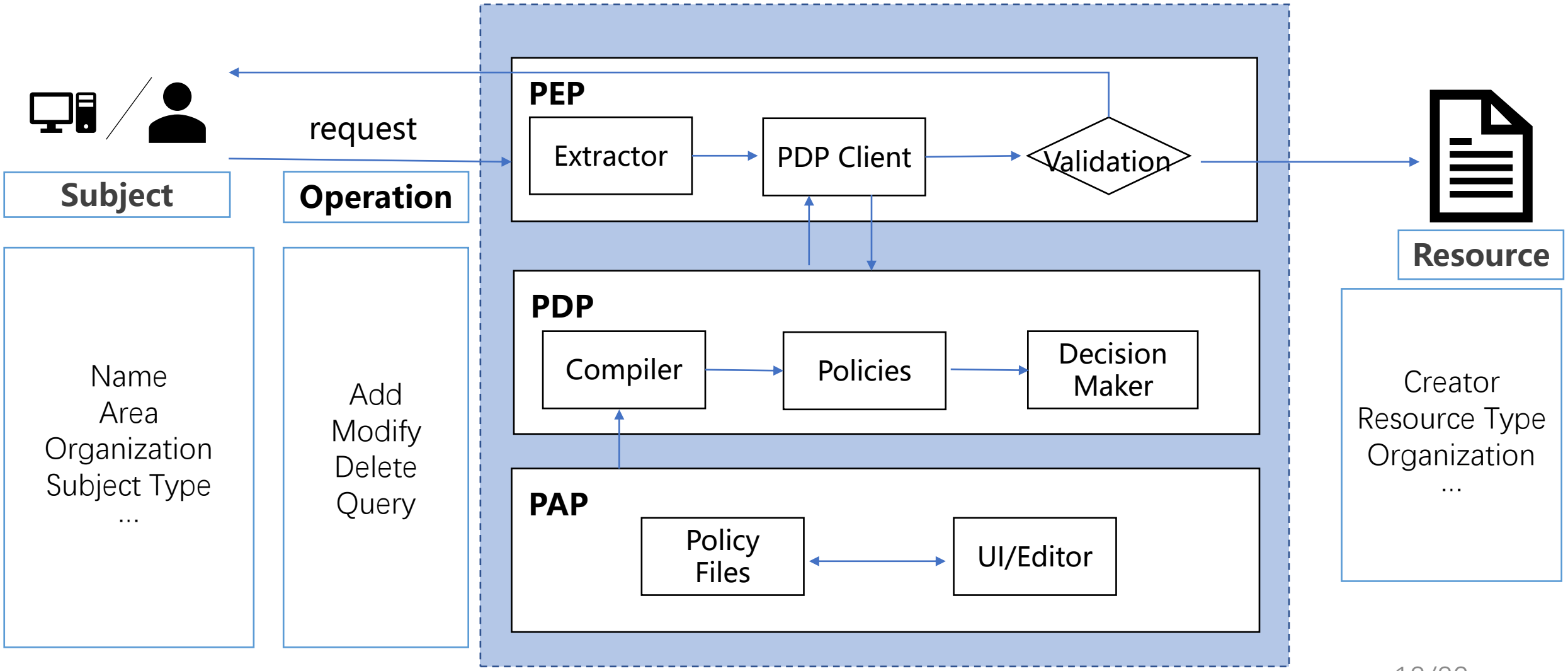
3. Solutions

Authorization

Technology	Advantage	Disadvantage	Problem With SWIM
DAC	Making decisions based on the subject's identity and access rights, with high flexibility	Authority of the subject is too large, information may be leaked unintentionally. The access control table ACL becomes large and difficult to maintain due to large number of users.	Large number of users in SWIM, making ACLs large and difficult to maintain
MAC	Strong security and strong control	Excessive emphasis on confidentiality, inconvenient management and low flexibility	Large workload for authorization policy formulation, Coarse control granularity
RBAC	Convenient for authorization management and Facilitating the processing of hierarchical management	No user and permission modification function, no operation sequence control mechanism	Difficult to change role of SWIM user
ABAC	High flexibility, Fine-grained control, Dynamic	Difficult to define attributes of subjects and resources	Suitable for SWIM

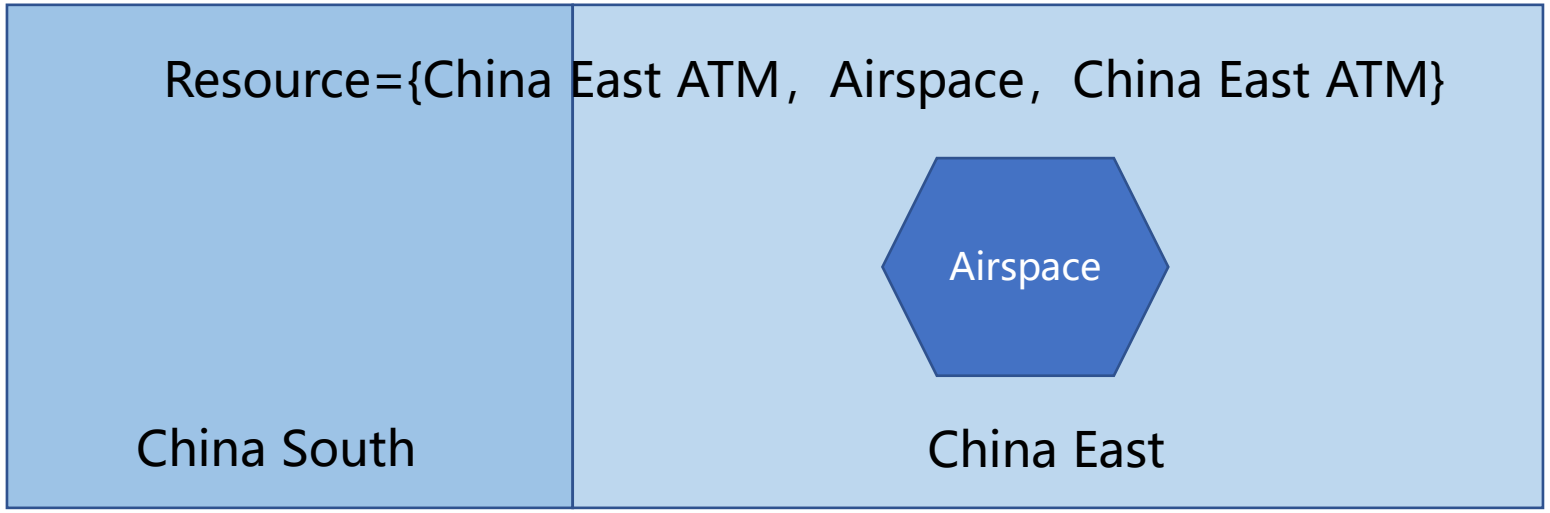
3. Solutions

Authorization—ABAC



3. Solutions

Authorization—ABAC



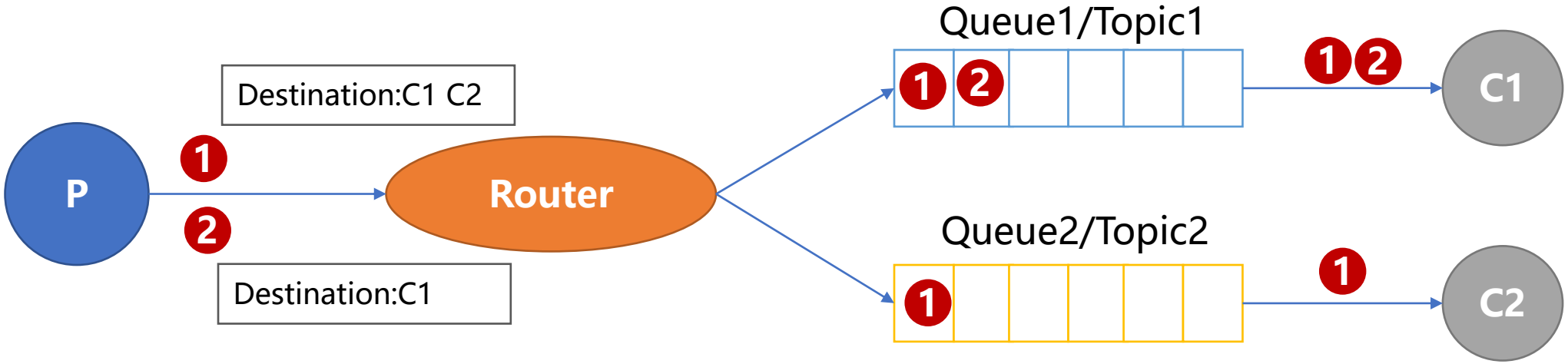
Subject1={China South ATM, China South, ATM, ATC System}

Policy={China_East_Area and ATM_Organization and (AMS_SubjectType,ATC System) 1of2}

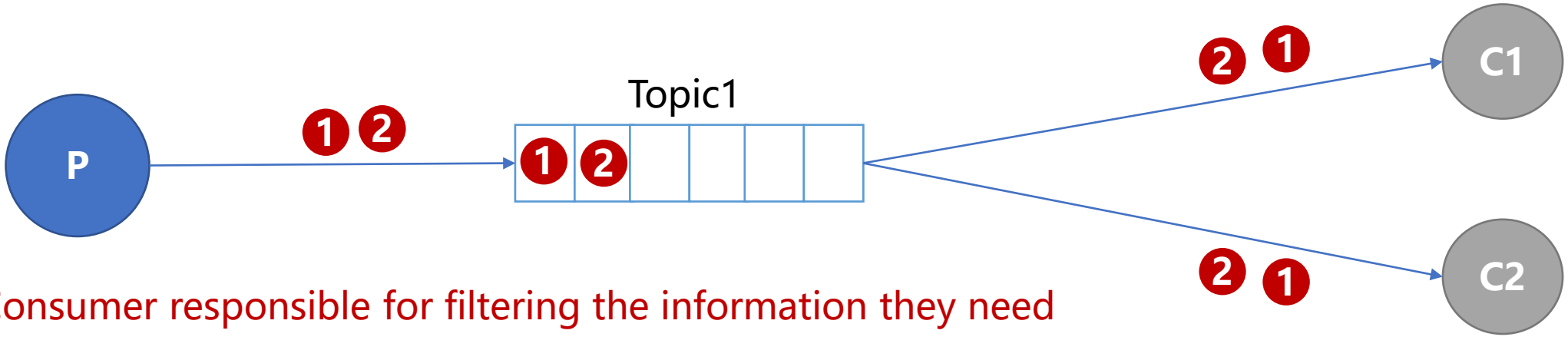
Subject2={China East ATM, China East, ATM, AMS}

3. Solutions

Another way to prevent data diffusion



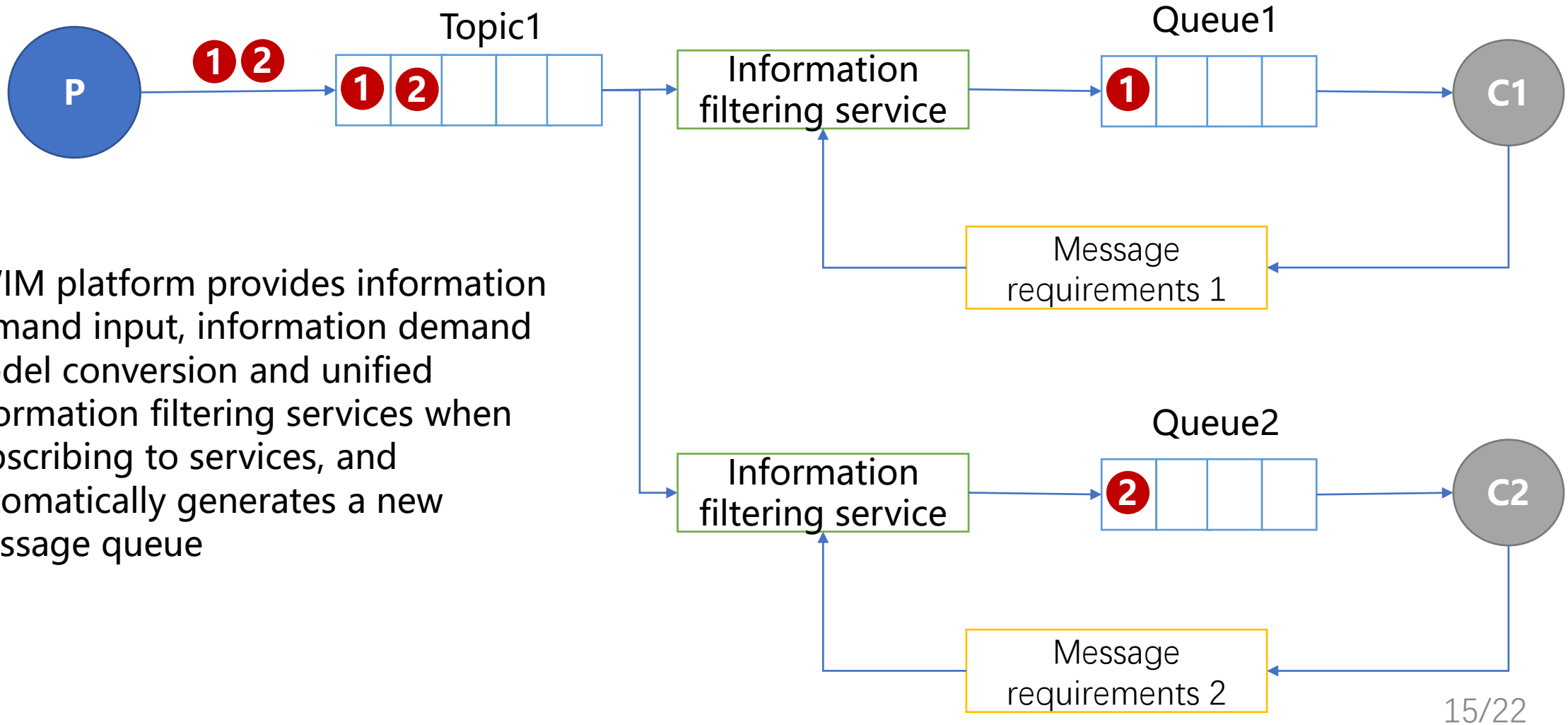
Provider responsible for controlling the scope of information dissemination



Consumer responsible for filtering the information they need

3. Solutions

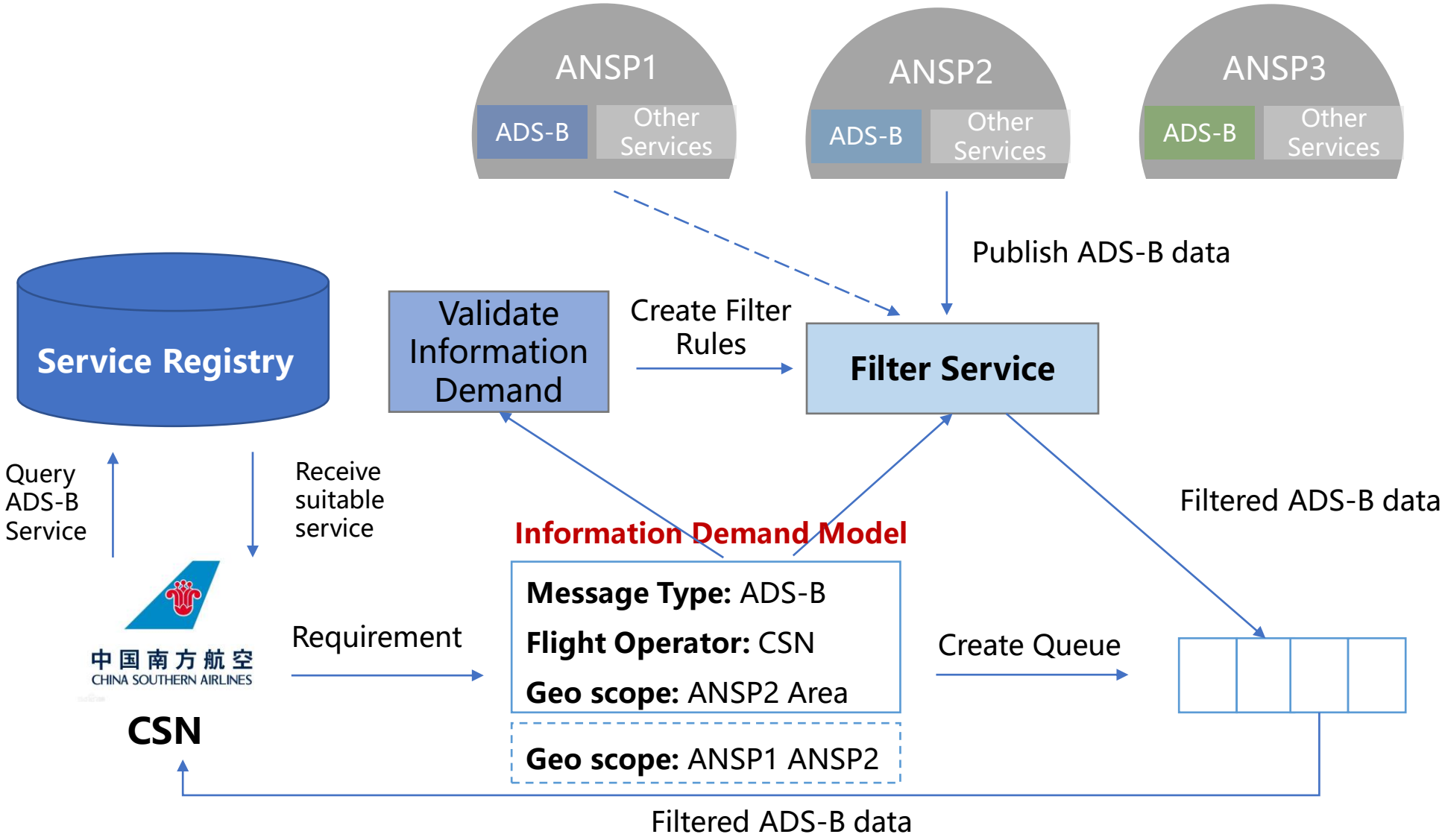
Another way to prevent data diffusion



SWIM platform provides information demand input, information demand model conversion and unified information filtering services when subscribing to services, and automatically generates a new message queue

3. Solutions

Another way to prevent data diffusion——Use Case



3. Solutions

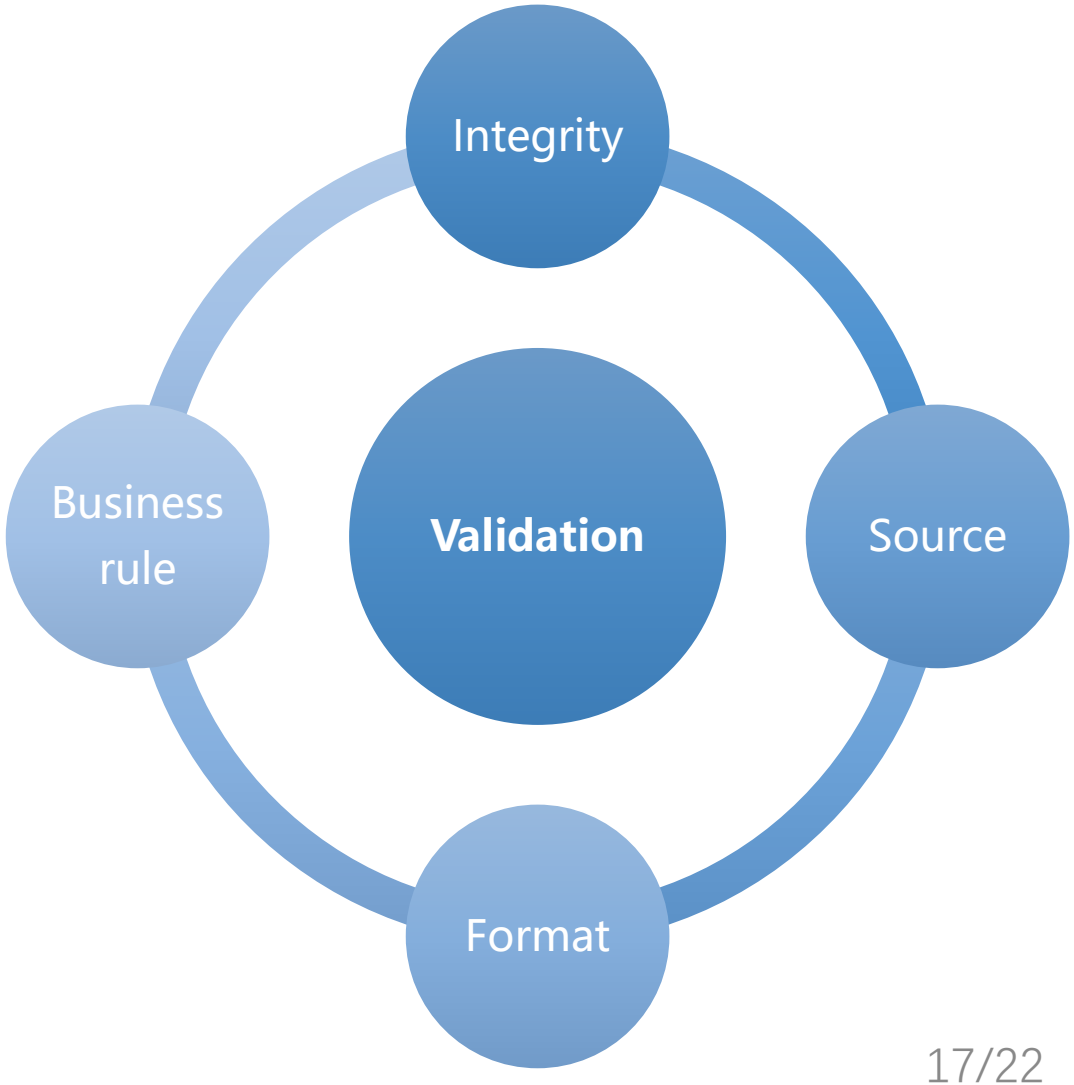
Information validation

Integrity validation: Information tampering validation

Source validation: Validate the consistency between the actual provider of the information and the declared provider

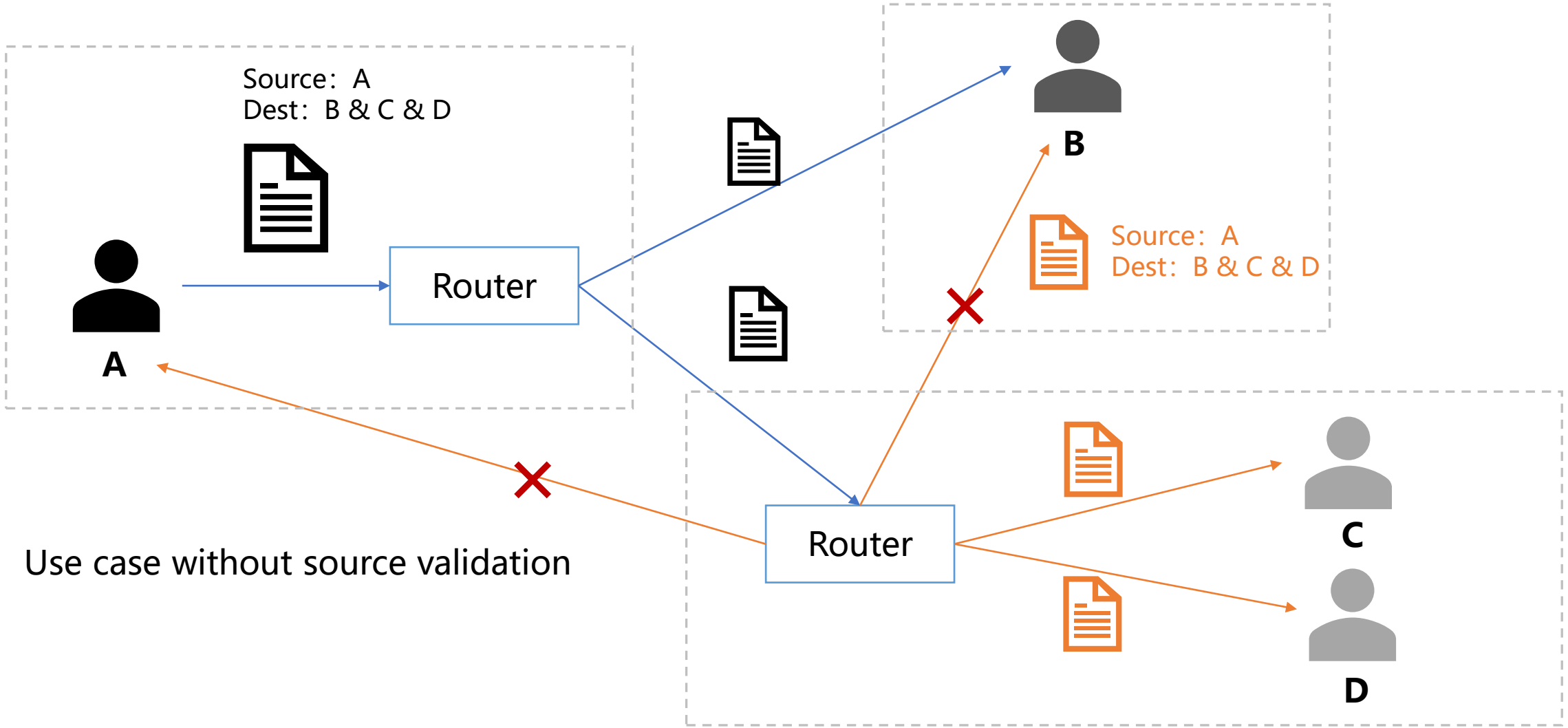
Format validation: Validate the consistency of the information and the information exchange model

Business rule validation: Validate the business logic of the information



3. Solutions

Information validation—Source Validation



Use case without source validation

3. Solutions

Information validation—Business Rule Validation (Flight Plan)

Version verification: low version information cannot over write high version information

Time verification: validation of the actual occurrence time and the information receiving time (the actual take-off time cannot be later than the information receiving time), and the associated time verification (take-off time and landing time)

Status verification: the plan status flight plan received later cannot be updated with the departure status flight plan

Other verification: coordinate system, height and speed range verification, etc.

Contents

4. Conclusion

Information transmission:
more secure and reliable

Authorization policy:
more flexible


Thank you!