SWIM TF/4 – **WP/09**
Agenda Item 5 (d) – Task 1-5
03 – 06/11/2020

International Civil Aviation Organization

The Fourth Meeting of System Wide Information Management Task Force (SWIM TF/4)

Web-conference, 3 – 6 November 2020

Agenda Item 5: Updates on the assigned tasks by task leads/contributors including progress Report and issues

d) Governance

- Registry - implementation guidance for Interoperable Registry Model
  - Task 5 (Contains previous Task 1-4, Task 1-5, Task 2-1-2, Task 2-1-4)

SECURITY AND TRUST IN THE CONTEXT OF SWIM SERVICE DISCOVERY

(Presented by FAA SWIM, USA, and Korea Airports Corporation (KAC), Republic of Korea)

SUMMARY

The joint FAA and KAC effort to develop a SWIM Discovery Service (SDS) specification (see WP/08) has demonstrated that an agreed-upon security and trust solution is a prerequisite for secure information exchanges between independently operated discovery services. Though high-level security requirements are identified in the SDS specification, they are rather a stop-gap solution that relies on pre-established trust. In this paper, we discuss options currently under consideration to secure SDS, and how the SDS effort can contribute to the establishment of a general SWIM security and trust framework for the Asia Pacific region (APAC).

1. INTRODUCTION

1.1 To facilitate exchange of service descriptions among independently operated SWIM programs, the US Federal Aviation Administration (FAA) and Korean Airports Corporation (KAC) collaboratively developed a specification for SWIM Discovery Service (SDS). [1]

1.2 Discovery services exchange descriptions about services published on their SWIM platforms. They communicate with one another through REST-style web services. One way to interact with SDS is through a SWIM registry. In that regard, SDS is the key enabler of the interoperable SWIM registry model adopted at the third SWIM TF meeting. [2]

1.3 Our work has identified interoperable security and trust solutions as essential for multiple SDS to exchange information. We have further demonstrated that security and trust issues in a diverse community like APAC SWIM need to be addressed from both the governance and the technical perspectives.

1.3.1 From the governance perspective, if states and Air Navigation Service Providers (ANSPs) in APAC want to form a peer-to-peer discovery network, business relationships will need to be established among themselves. This may involve bilateral or multilateral service level agreements (SLA), which may also require the Task Force to define relevant governance policies.

1.3.2 From the technology perspective, standards and protocols should be specified to describe and enforce the trust relationships.

1.4 The current SDS specification includes only high-level authentication and access control requirements. Though this stop-gap solution will be applicable to a limited number of services, a more comprehensive solution is required. This paper aims to bring the attention of APAC security experts and integrators to the issues that we encountered in the service discovery area and to the potential use of our model as a case study.

2. SECURITY AND TRUST FROM GOVERNANCE AND TECHNICAL PERSPECTIVES

2.1 The security and trust issues associated with SDS can be illustrated using the example shown in Figure 1. Note: “discovery service” is abbreviated as “DS” in the remainder of this paper.

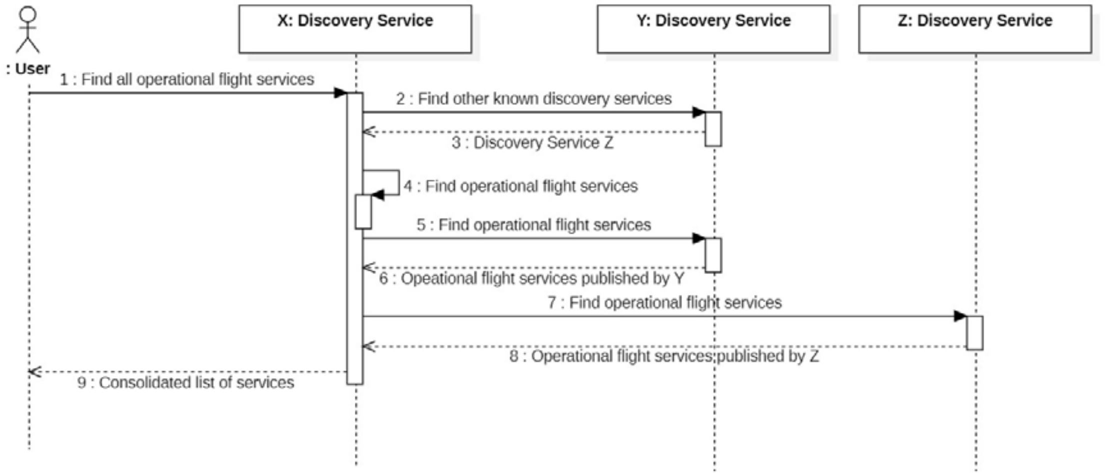
: User
X: Discovery Service
Y: Discovery Service
Z: Discovery Service
1 : Find all operational flight services
2 : Find other known discovery services
3 : Discovery Service Z
4 : Find operational flight services
5 : Find operational flight services
6 : Opeational flight services published by Y
7 : Find operational flight services
8 : Operational flight services published by Z
9 : Consolidated list of services

Figure 1 Use case for finding all operational flight services

2.1.1 In this example, the user has access and necessary security credentials to a DS (labeled “X” in Figure 1). DS X has an established relationship with Y, which in turn has a relationship with Z.

2.1.2 The scenario starts when the user requests X to “find operational flight services” from all SWIM programs in the region.

2.1.3 In response to this request, X first attempts to discover additional DSs in the region. It learns of the existence of Z from Y.

2.1.4 X then queries its own database as well as both Y and Z. X consolidates responses from all three sources and presents the user with a single list.

2.2 This scenario raises questions about the relationships among the DSs. For example,

2.2.1 Are all DSs required to trust one other? In our example, X only discovers the existence of Z through Y. Should there be any bilateral agreement between X and Z?

2.2.2 How does a DS advertise its security requirements? For example, Z could make its authorization decisions based on the identity of X, the end user, or a combination of both.

2.2.3 What responsibility does a DS have when it acts as an intermediary? For example, could Z limit its visibility to certain other DSs? In this case, Y would only inform X about Z’s existence when certain criteria are met.

2.2.4 How does a DS assess the accuracy and completeness of information provided by another DS? In our example, X is likely to indicate in its consolidated response to the user that certain service descriptions are from sources outside its control.

2.3 This scenario also raises questions about the relationship between a DS and the end user. For example,

2.3.1 From the business perspective, it is reasonable to assume that a DS wants to know the identity of the ultimate recipient of information – the user. How does X pass the user identity to Y and Z without requiring separate accounts to be established?

2.3.2 From the access control perspective, a DS may limit distribution of information based on the identity of the user. Should a common list of user attributes be defined to ensure interoperability among DSs in a region?

2.4 This scenario highlights the interaction points where authentication may be required, including between the end user and the DS, and among the DSs themselves. For example,

2.4.1 When the user requests X to “find all operational flight services”, X may need to identify the user prior to authorizing access.

2.4.2 When X forwards a request to another DS, the other DS may need to authenticate X and validate its trust relationship with X prior to producing a response.

2.4.3 Even if a trust relationship exists between X and the other DS, the other DS may need to identify the ultimate recipient of information – the user. It may enforce access control policy based on the identity of the user.

2.4.4 Though we have identified all authentication points, it is possible that a given use case may require only a subset of them to be implemented.

3 A NOTIONAL IMPLEMENTATION APPROACH

3.1 FAA and KAC are investigating a federated identity management solution to secure the communication between our discovery service implementations. In this approach, the end user is registered as a domain user of a DS. Federated identity management technologies such as OAuth [3] or Security Assertion Markup Language (SAML) [4] can be used to exchange user identity information between the DSs.

3.2 With this notional implementation approach, we can answer the questions raised in sections 2.2 and 2.3 as the following:

3.2.1 **[Q]** Are all DSs required to trust one other?

[A] Currently all information available via a SWIM registry is open and freely available, and it is expected that a DS may also publish only openly available information. Information exchanges between DSs which are compliant with the SDS specification are conducted under the assumption that there is mutual agreement between DSs.

3.2.2 **[Q]** How does a DS advertise its security requirements?

[A] Each DS is able to obtain the security requirements of another DS through a `GetDiscoveryService` operation. Examples of security requirements include the use of a token or ID/password.

3.2.3 **[Q]** What responsibility does a DS have when it acts as an intermediary?

[A] The answer depends on whether a DS intends to provide services to all other DSs (that is, if it has a public open policy). In our example, if Z is only accessible from Y, then validating the information provided by Z becomes Y's responsibility.

3.2.4 **[Q]** How does a DS assess the accuracy and completeness of information provided by another DS?

[A] A response to a `GetServices` operation may include an “original source” attribute or any other attribute needed to enhance integrity of information (e.g., “date of last update”).

3.2.5 **[Q]** From the business perspective, is it reasonable to assume that a DS wants to know the identity of the ultimate information consumer – the user?

[A] Only users who are identified, authenticated, and authorized are able to use a DS, and there is no need to share user’s identification between DSs. In other words, the DS invoked by the user should be responsible for granting the user access.

3.3 The SWIM Concept (Doc 10039) [5] states that the objective of a SWIM service registry is to publicize available information services and discover their corresponding service overviews. Since the purpose of a DS is to exchange information about a service and advertise it, the security mechanisms and procedures required for exchange between DSs need to be simplified.

4 OVERVIEW OF RELEVANT SECURITY TECHNOLOGIES

4.1 The Information Technology (IT) industry has made significant progress in building trust relationships among heterogeneous systems. In order to determine the appropriate authentication mechanism between DSs, security technologies commonly used in the industry should be considered.

4.2 There are several security technologies in the industry. For example, Identity and Access Management (IAM) is a mature and commonly used security technology. Identity as a Service (IDaaS) or Blockchain based Decentralized Identifiers (DID), on the other hand, are currently a promising security technology that can implement a decentralized security mechanism. A brief introduction of these technologies is as follows:

4.2.1 Identity and Access Management (IAM) is an authentication system that uses Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), or Active Control (AC). IAM is a system commonly used to implement security in the IT industry and provides various authentication methods such as password, token, X.509 credential, and form-based authentication.

4.2.2 Identity as a Service (IDaaS) is an authentication infrastructure built and managed by a third-party service provider. IDaaS companies provide cloud-based authentication or identity management to enterprise subscribers. It allows enterprises to use single sign-on, authentication, and access controls to provide secure access to their growing number of software and SaaS applications.

4.2.3 Based on Distributed Ledger Technology (DLT) or blockchains, Decentralized Identifiers (DID) provides authentication mechanism without a central authority. Instead of delegating identity check to an external authority, it enables Self-Sovereign Identity (SSI), which allows users to prove their identity themselves. Though it is a relatively new security technology, there are already several blockchain projects in the aviation industry. United Airlines has completed a proof of concept with Airlines Reporting Corporation (ARC) for the use of blockchain technology to report and settle airline tickets[6], and Korea's Incheon Airport and China's Tianjin Airport Korea's Incheon Airport has conducted a pilot project with Samsung SDS to exchange air cargo data using blockchain network between two airports[7].

5 RELATIONSHIP WITH PROPOSED APAC MUTUAL TRUST INFRASTRUCTURE

5.1 Through collaboration with the Security Management subtask (Task 5), FAA and KAC understand that an APAC Mutual Trust Infrastructure is being developed. The proposed infrastructure requires individual states and ANSPs to establish PKI and uses a blockchain to facilitate interoperability. [8]

5.2 However, we understand that a mutual security framework for identification and authentication (i.e., trust relationship) between DSs is required. It would be inappropriate to create a security framework only for DSs, and it is likely that DSs would use the APAC Mutual Trust Infrastructure.

5.3 We believe this paper raises the issue of trust between DSs to the SWIM TF. This issue is not simply an issue that needs to be covered within the registry task; it seems to us that collaboration with the security task is necessary as this issue could arise in any other global SWIM services which require identification, authentication, and authorization of user and system.

5.4 It is conceivable that the proposed Infrastructure can be extended to allow authentication of individual users following the verifiable credentials approach [9] supported by the blockchain. In this case, a set of standard user assertions needs to be developed jointly by the security task and the governance task. These assertions will be used by a DS to make access control decisions. In addition, it is expected that the impact of this issue on other global SWIM services should be considered, and if it is required, the TF should analyze it and develop a solution.

6 FUTURE CONSIDERATIONS FOR THE TASK FORCE

6.1 It is suggested that some issues raised in this paper be addressed within the Task Force Governance Task (Task 4), consistent with the APAC Policy-Centric Governance Model [10]. These issues include:

- Standards and policies for a DS to advertise its security and trust requirements;
- Standards and policies for a DS to add security and trust metadata to service descriptions.

6.2 A generalized discussion on security issues including authentication for SWIM services should be conducted, and it is suggested that TF governance task and the TF security management task further collaborate and consider the next steps.

7 ACTION BY THE MEETING

7.1 The meeting is invited to:

a) Review the contents of this Working Paper;

b) Consider the recommendations outlined in Section 6;

c) Encourage further collaborations on the technical approach proposed.

8 REFERENCES

[1] FAA and KAC, “SWIM Discovery Service (SDS)”, WP/XXX, ICAO SWIM Task Force/4, November 2020

[2] KAC, “APAC SWIM Registry Approach”, WP/16, ICAO SWIM Task Force/3, May 2019 https://www.icao.int/APAC/Meetings/2019SWIMTF3/WP16_ROK%20AI3%20-%20SWIM%20Registry%20Approach%20Revised.pdf

[3] Hardt, Dick. The OAuth 2.0 authorization framework. RFC 6749, October, 2012. https://tools.ietf.org/html/rfc6749

[4] Cantor, Scott, et al. "Metadata for the OASIS security assertion markup language (SAML) V2.0", 2005 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[5] Bing Leng, “Blockchain Based Mutual Trust Infrastructure Building among APAC States”, WP/ XXX, ICAO SWIM Task Force/4, November 2020

[6] Applying Blockchain to Air Travel
https://www2.arccorp.com/articles-trends/the-latest/applying-blockchain-to-air-travel/

[7] Samsung SDS Expands Blockchain Business with cloud-based Enterprise Platform
https://www.samsungsds.com/global/en/about/news/Samsung-SDS-Expands-Blockchain-Business-with-Cloud-based-Enterprise-Platform.html

[8] ICAO, “MANUAL ON SYSTEM WIDE INFORMATION MANAGEMENT (SWIM) CONCEPT." Doc 10039, 2015.

[9] World Wide Web Consortium, “Verifiable Credentials Data Model 1.0”, W3C Recommendation, November 2019
https://www.w3.org/TR/vc-data-model/

[10] FAA, “Policy-Centric Governance Model for APAC SWIM”, WP/09, ICAO SWIM Task Force/2, May 2018
https://www.icao.int/APAC/Meetings/2018%20SWIMTF2/WP09%20Task%201-4%20-%20Policy-Centric%20Governance%20Model%20for%20APAC%20SWIM.pdf

– – – – – – – – – – – – – – –