WP 09: SECURITY AND TRUST IN THE CONTEXT OF SWIM SERVICE DISCOVERY

Task 1-5 Governance

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

Presented by: Federal Aviation Administration (FAA), USA
Korea Airports Corporation (KAC), ROK

03 – 06 November 2020

1. Introduction

- Security and trust is a prerequisite for secure exchanges
  - Lessons learned from SWIM Discovery Service (SDS) collaboration (See WP/08)
- Security from governance and technical perspectives
  - Relationships/agreements among peers
  - Standards/protocols to secure information exchanges
- Our experience as a case study
  - Current stop-gap solution with pre-established trust

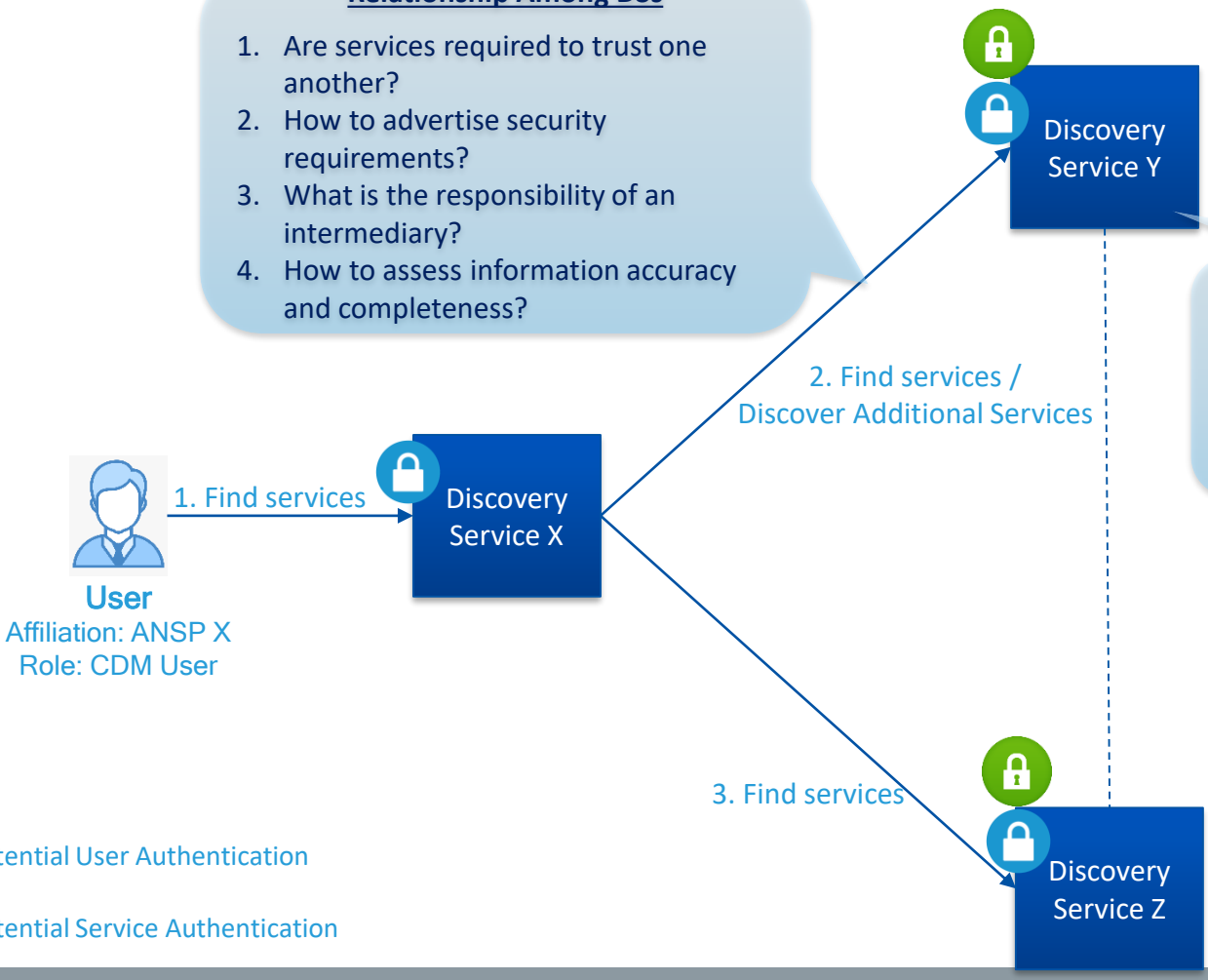
2. Governance and Technical Perspectives

Relationship Among DSs

1. Are services required to trust one another?
2. How to advertise security requirements?
3. What is the responsibility of an intermediary?
4. How to assess information accuracy and completeness?

Relationship between User and DS

1. How is user's identity passed?
2. What are the common attributes required for access control?



3. A Notional Implementation Approach

- Future Implementation of a Discovery Service?
  - Multiple DSs operated by different enterprises or states
  - Stakeholders from different organizations access to DS

    - Federated Identity Management (FIM) : the set of agreements and standards that enable the identities across multiple enterprises and large numbers of users

    - Security mechanisms required for exchange between DSs need to be simplified, as the objective of a SWIM service registry is to publicize available services and discover corresponding service overviews. And 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.

3. A Notional Implementation Approach

- Answers to the questions raised in section 2

Are all DSs required to trust one other?

Information exchanges between DSs which are compliant with the SDS specification are conducted under the assumption that there is mutual agreement between DSs.

How does a DS advertise its security requirements?
How does a DS assess the accuracy and completeness of information provided by another DS?

SDS already includes or may include attributes for them

3. A Notional Implementation Approach

- Answers to the questions mentioned in section 2

What responsibility does a DS have when it acts as an intermediary?

For example, Z is only accessible from Y, then validating the information provided by Z becomes Y's responsibility.

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

The DS invoked by the user should be responsible for granting the user access

4. Overview of Relevant Security Technologies

- Information Technology (IT) industry has made significant progress in building trust relationships among heterogeneous systems
- Security technologies can be considered for building trust between DSs:
  - Identity and Access Management (IAM)
  - Identity as a Service (IDaaS)
  - Distributed Ledger Technology (DLT)

5. Relationship with Proposed APAC Mutual Trust Infrastructure

- APAC SWIM TF is working on developing an APAC Mutual Trust Infrastructure
- It is plausible for DS to use it instead of implementing a security framework only for DSs
- Security and trust relationship issue raised also could arise in any other global SWIM services

6. Recommended Future Consideration for TF

- Governance Task (Task 5)
  - 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
- Collaboration between Governance and Security Services Tasks (Task 3)
  - Generalized discussion on security issues including authentication for SWIM services

7. Actions by the Meeting

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