



**INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE**

**REPORT
OF
ASIA PACIFIC REGIONAL CYBERSECURITY WEBINAR**

Video Tele-Conference (VTC)
14 June 2021

The views expressed in this Report should be taken as those of
the Webinar and not the Organization.

Published by the ICAO Asia and Pacific Office, Bangkok

HISTORY OF THE WEBINAR	Page
1. Introduction	1
2. Attendance	1
3. Opening of the Webinar	1
4. Officers and Secretariat	1
5. Organization, working arrangements and language.....	1
6. Summary of Presentations	1
7. Closing of Webinar	2

LIST OF ATTACHMENTS

- Attachment 1:** Webinar Programme
- Attachment 2:** Presentation materials + Q&A
- Attachment 3:** List of Participants

1. Introduction

1.1 The ICAO Asia Pacific Regional Cybersecurity Webinar was held on *14 June 2021*. The webinar was organised via Video Tele-Conferencing (VTC) using Microsoft Teams.

2. Attendance

3.1 The Webinar was attended by **317** participants from **26** States/Administrations (Afghanistan, Australia, Bangladesh, Bhutan, Brunei Darussalam, China, Hong Kong China, Macao China, Fiji, India, Indonesia, Japan, Lao, Malaysia, Nepal, New Zealand, Pakistan, Philippines, Republic of Korea, Singapore, Sri Lanka, Timor-Leste, Thailand, USA and Viet Nam), **6** International Organizations (AAPA, CANSO, IATA, ICANN, IFALPA, and IFATCA) and **2** Technology/Solutions providers (Nokia and Thales) who sponsored the event. The list of participants is provided in **Attachment 3**.

3. Opening of the Webinar

3.1 The Webinar was opened by Mr. Manjit Singh, Acting Regional Director, ICAO Asia and Pacific Office. Mr. Manjit Singh extended warm welcome to all participants and expressed his thanks to States/Administrations and to the Aviation Industry's Safety and Security Partners for the continuous support to ICAO Regional Activities. He expressed that the webinars are an excellent platform to share information and experience under the influence of the outbreak of the COVID-19 pandemic. Furthermore, he emphasized that the cyber threats are currently growing at an increasing rate and becoming a pertinent concern to Civil Aviation as increasing IP-based network connectivity and new concepts such as System-wide Information Management (SWIM) are making us more connected and also integrated as a single operating global network. Given the dynamic nature of cyber threats to the Air Navigation, airport and other critical aviation systems, it is time for all relevant entities in the National and International levels to work collaboratively in order to provide a more proactive and aligned collective response to Cyber Threats through a cross-cutting approach. He also recalled the achievements of first APAC Regional Cybersecurity Symposium and the recommendation of CNS SG/24 held in November 2020 to build regional capability about cybersecurity-related challenges and emphasized the need for members to share information and experience, develop awareness on cyber issues affecting aviation, and foster a cyber-safety culture that promotes a resilient and secure cyberspace.

4. Officers and Secretariat

4.1 Mr. Luo Yi, Regional Officer, CNS and Ms. Soniya Nibhani, Regional Officer, ANS (CNS) Implementation of ICAO Asia and Pacific Regional Office acted as the Moderators of the Webinar with the support of Mr. How Sze Lung, Associate CNS Officer, Ms. Zhong Wenhan, Associate CNS Officer, and Ms. Bhabhinan Sirapongkosit, the Programme Assistant of the same office. The Webinar were organised in Three Sessions. Mr. How Sze Lung, Associate CNS Officer operated Pigeonhole Q&A throughout the Webinar. The Programme for the Webinar is provided in **Attachment 1**.

5. Organization, working arrangements and language

5.1 The Webinar was conducted via Video Tele-Conferencing (VTC) using Microsoft Teams platform supported by Pigeonhole tool for Q&A. The working language was English inclusive of all documentation and this Report.

6. Summary of Presentations

6.1 Total **Ten** (10) presentations were delivered by Experts from different part of the World under different Domains related to Cyber Security. The presentation materials along with corresponding Q&A from the Webinar are provided as **Attachment 2** to this report. The presentation materials can also be accessed by the link: <https://www.icao.int/APAC/Meetings/Pages/2021-Cyber->

[Security-Webinar.aspx](#). The summaries of all presentations are as follows:

SP101 – ICAO Trust Framework Latest Development

6.2 Ms. Olga De Frutos Martin and Mr. Michael Goodfellow, Technical Officers from Air Navigation Capacity and Efficiency (AN), Air Navigation Bureau, ICAO, also the secretaries of the ICAO Trust Framework Study Group (TFSG), informed in the Webinar about the latest updates in the International Aviation Trust Framework which is being developed by ICAO, including the information security framework as well as digital identity management system.

SP102 – FAA's contribution to the IATF and Importance of IATF to FAA

6.3 Mr. Robert Segers, National Airspace System (NAS) Information Systems Security Architect of Federal Aviation Administration, and Member of the ICAO TFSG, introduced the latest contributions of the FAA to the validation of the International Aviation Trust Framework as well as the importance of this Trust Framework to FAA.

SP103 – Cyber Safety in ATM

6.4 Mr. Shayne Campbell, Safety Programme Manager of CANSO, shared their recently launched Standard of Excellence in Cybersecurity, which helped ANSPs assess, develop and improve their cybersecurity to provide safe and resilient air navigation services. The presentation introduced how ANSPs prepare themselves to secure their systems and adopt all necessary measures to ensure the continuous provision of highly safe and seamless air traffic services.

SP201 – Protecting All Systems

6.5 Mr. John Moore, Assistant Director, Safety and Flight Operations – ASPAC, International Air Transport Association (IATA), established a picture of the IATA's efforts in providing support to their members in protecting their systems and expecting the robustness and reliability of CNS/ATM systems as the important data source for operation.

SP202 – DNS Ecosystem Security

6.6 Mr. Champika Wijayatunga, Technical Engagement Manager – Asia Pacific, Internet Corporation for Assigned Names and Numbers of ICANN, joined ICAO APAC regional discussion platform for the first time. He expounded on the critical role of The Domain Name System (DNS) in the Internet infrastructure, the overview of the DNS Ecosystem, various threats and abuses in the DNS and the best practices in protecting the DNS.

SP203 – Building Mutual Trust Infrastructure Based on Blockchain

6.7 Mr. Leng Bing, Principal Researcher, Southwest Communications Institute of China, introduced a proposed method to build mutual trust among States in the Asia Pacific region by using blockchain technology. The use of blockchain could give inspiration to find a way out under the current global governance.

SP301 – A proactive and systematic approach in protecting digitized air traffic services against cyber threats in Hong Kong from ANSP and regulatory perspective

6.8 Mr. Raymond Chan, Senior Electronics Engineer, Civil Aviation Department of Hong Kong, China, shared the cybersecurity practices in Hong Kong Civil Aviation Department to protect its highly digitized air traffic services systems from both service provider and regulatory perspective.

SP302 – Air Traffic Management Security and Updates on ICAO Cybersecurity Activities

6.9 Mr. Remington Low, Regional Officer FAL, Asia Pacific Regional Office of ICAO explained the ICAO security requirements on ANSPs and ATM, and the update of the Cybersecurity Action Plan and the Secretariat Study Group on Cybersecurity.

SP303 – A Security Solution for Information Services in SWIM

6.10 Mr. Tian Yungang, Section Chief, State Key Laboratory of Air Traffic Management System and Technology of China, introduced their research on the security architecture of SWIM information services and security measures to improve the security assurance capabilities of SWIM information sharing.

SP304 – Cybersecurity – A vendors perspective

6.11 Mr. Binny Sarien, Security Design Authority, Thales Australia – Airspace Mobility Solutions, introduced the view from Thales as a leading solution and service provider to ANSPs in the cybersecurity domain. This presentation summarized cybersecurity from a vendors' perspective, highlight key situational awareness aspects and describe what makes a good cyber solution for ANSPs,

7. Closing of Webinar

7.2 On behalf of the ICAO Secretariat, Mr. Luo Yi, Regional Officer CNS concluded the Webinar. He summarised the key message from each presentation and extended sincere gratitude to all Speakers for joining the Webinar and to share the information with APAC Member States. He also expressed appreciation and gratitude to the NOKIA and THALES to sponsor the event. He further explained that considering the restriction of online mode and the time zone challenges for the Speakers, no panel discussion was set up and no Conclusions or Decisions being formulated by this Webinar.

7.3 In addition, Mr. Luo Yi reiterated that Capacity building on Cybersecurity Awareness from Member States is an endless process as long as we continue to exchange Information in Cyberspace. Therefore, this webinar is a good practice to improve each individual as a human firewall with good awareness of Cyber Security and Cyber Safety. He concluded that such huge number of participants indicates the need to organize such kind of Webinars/Events in future. Participants were assured that ICAO APAC Office will continue this joint effort with all stakeholders.

7.4 During the Webinar, Questions and Answers (Q & A) sessions were held at end of each presentation through the Pigeonhole tool. Throughout the Webinar, a total of **69 questions** were asked and *more than 100 feedback* for the Webinar were provided by Participants with **100% positive response**.



ICAO

ICAO Asia/Pacific Regional Cybersecurity webinar

Management Framework for CNS/ATM Systems

14 June 2021 (UTC+7)

Opening Session

Note: All times indicated are in Bangkok Local Time (UTC+7)

08:00 – 08:05	Inauguration <i>Mr. Manjit Singh , Acting Regional Director</i>
08:05 – 08:10	Introduction ✓ Introduction of Participants Logistics information ✓ Administrative information ✓ Pigeonhole tool instructions Please download all documents/presentations here . Please download your Virtual Delegate Bag here .
Session 1	
08:10 – 09:50	Moderator- <i>Mr. LUO Yi, Regional Officer, CNS</i> 1. SP101 – ICAO Trust Framework Latest Development <i>Ms. Olga De Frutos Martin and Mr. Michael Goodfellow</i> Technical Officers, Air Navigation Capacity and Efficiency (AN), Air Navigation Bureau, International Civil Aviation Organization (ICAO) Question and Answer 2. SP102 – FAA’s contribution to the IATF and Importance of IATF to FAA <i>Mr. Robert Segers</i> NAS Information Systems Security Architect, Member of the ICAO Trust Framework Study Group, Federal Aviation Administration Question and Answer 3. SP103 – Cyber Safety in ATM <i>Mr. Shayne Campbell</i> Safety Programme Manager, CANSO Question and Answer
09:50 – 10:10	Refreshment Break + Looping Video by NOKIA



ICAO

ICAO Asia/Pacific Regional Cybersecurity webinar

Management Framework for CNS/ATM Systems

14 June 2021 (UTC+7)

Session 2

10:10 – 11:50	Moderator- <i>Ms. Soniya Nibhani, Regional Officer, ANS (CNS) Implementation</i> 4. SP201 – Protecting All Systems <i>Mr. John Moore</i> <i>Assistant Director, Safety and Flight Operations-ASPAC, International Air Transport Association (IATA)</i> Question and Answer
	5. SP202 – DNS Ecosystem Security <i>Mr. Champika Wijayatunga</i> <i>Technical Engagement Manager – Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN)</i> Question and Answer
	6. SP203 – Building Mutual Trust Infrastructure Based on Block Chain <i>Mr. Leng Bing</i> <i>Principal Researcher, Southwest Communications Institute of China</i> Question and Answer
11:50 – 12:35	Lunch break



ICAO

ICAO Asia/Pacific Regional Cybersecurity webinar

Management Framework for CNS/ATM Systems

14 June 2021 (UTC+7)

Session 3	
12:35 – 14:45	Moderator- <i>Ms. Soniya Nibhani, Regional Officer, ANS (CNS) Implementation</i> 7. SP301 – A proactive and systematic approach in protecting digitized air traffic services against cyber threats in Hong Kong from ANSP and regulatory perspective <i>Mr. Raymond Chan</i> <i>Senior Electronics Engineer, Civil Aviation Department (CAD), Hong Kong, China</i> Question and Answer
	8. SP302 – Air Traffic Management Security and Updates on ICAO Cybersecurity Activities <i>Mr. Remington Low</i> <i>Regional Officer FAL, Asia/Pacific Regional Office, International Civil Aviation Organization (ICAO)</i> Question and Answer
	9. SP303 – A Security Solution for Information Services in SWIM <i>Mr. Tian Yungang</i> <i>Section Chief, State Key Laboratory of Air Traffic Management System and Technology, China</i> Question and Answer
	10. SP304 – Cybersecurity – A vendors perspective <i>Mr. Binny Sarien</i> <i>Security Design Authority–Thales Australia – Airspace Mobility Solutions</i> Question and Answer
Closing Session	
14:45 – 15:00	11. Review Outcomes from Webinar and Closing Remarks <i>Mr. LUO Yi</i> <i>Regional Officer, CNS</i>



ICAO

UNITING AVIATION

Attachment 2 to the Report

INTERNATIONAL AVIATION TRUST FRAMEWORK (IATF)

Bangkok
June 2021





Flight Plan

- Introduction
- What is the IATF?
- Digital Identity
- Network
- Conclusion



MULTILAYER STRUCTURE OF THE GANP

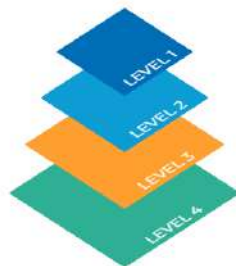
Click a level to navigate

GLOBAL STRATEGIC

GLOBAL TECHNICAL

REGIONAL

NATIONAL



- **Information: Key for evolution**
 - Global information utilization, management and interchange
 - Aviation is moving towards the notion of full connectivity
- **Technical level:**
 - More automation
 - Digitalization of the air navigation system based on a service oriented architecture
 - Performance-driven towards a more cost-effective system
- **Places a premium on:**
 - The performance of data and information
 - Information security

<https://www4.icao.int/ganpportal/>



A converging strategy

- Interoperability requires global coordination and cooperation
- Identify common needs that can unite all aviation ecosystem stakeholders
- Develop common solutions that build on existing foundations
- Agree on a common destination – where there is still one interoperable sky

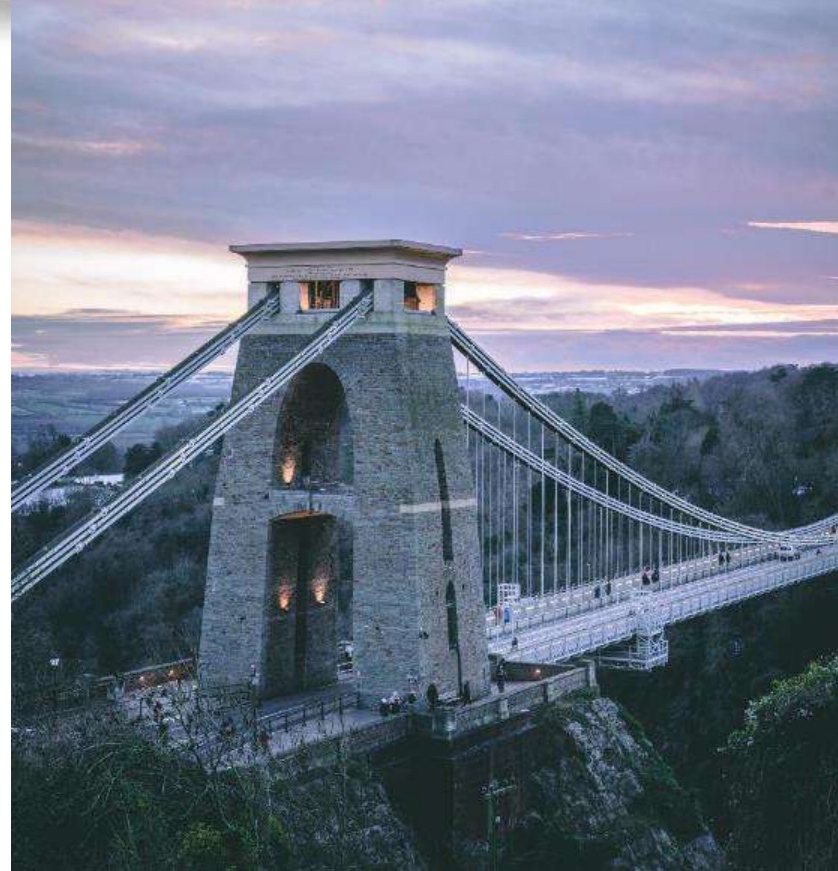


What is the IATF?

- A framework to reduce the cyber-attack surface and enable reliable and trusted exchange of information for aviation using the Internet infrastructure.

Trust Framework – A Common Solution

- Foundation - International Law
 - Chicago Convention, Beijing Convention (Article 21), Annexes, etc...
- Trusted Digital Identity
 - Anchored in proven regulatory processes
- Trust Bridge
 - Allows identities to be recognized across boundaries





ICAO

UNITING AVIATION

Trust framework

- The foundational principle of the global aviation system that connects us today
- A core function of ICAO since 1944
- An evolution of this framework now seems essential
 - Based on common standards
 - Anchored in State sovereignty
 - Facilitating global recognition of digital identities
 - Applied consistently across the aviation ecosystem





Credibility Flows from the Regulator

- Regulators spend countless hours interacting with all the components of the aviation ecosystem
- Once aircraft, facilities, or services operate under the State's oversight, the world can trust that assertion



Examples:

- Aerodromes
- Air Operators
- Aviation Maintenance Organizations
- Producers of aircraft, engines, propellers and parts
- Air Traffic Service Provision
- MET Service Provision
- AIS Service Provision
- Communication Facilities
- Design of aircraft, engines and propellers
- RVSM Monitoring Agencies
- Personnel
- **Remotely Piloted Aircraft Systems**
- **Unmanned Traffic Management (UTM)**
- **Upper class E Traffic Management (ETM)**
- **Future Autonomous Systems?**



Which are its components?

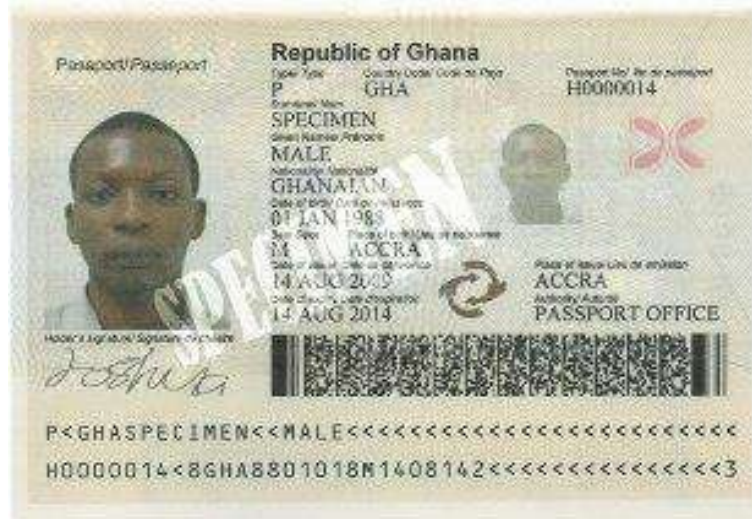
- Digital Identity
- Network information security



Identity

- Provides information (**contents**) to answer the question “who/what are you?”
- Presents itself in a readable form (**credential**) that can be independently validated or proven, and carries a certain level of trust or recognition (**assurance**)

Example - Passport



- Is a **credential** that can be validated
- Has **contents** that describe the owner
- Provides a certain level of **assurance** the identity is valid



Digital Identity

- Digital identity is the digital equivalent of physical/personal identity
 - Says who or what you are
 - Provides a credential to validate
 - Asserts that credential to a given level of assurance



Digital Identity Usage

- Digital identity relies on easily usable, simple to validate and difficult to reproduce/forged **electronic credentials**
- Digital identity credentials have multiple uses:
 - Documents / Certificates for personnel and aircraft (ID badges, licenses, CoA, CoR, etc...)
 - Message validation (SWIM, ACARS Message Security, etc...)
 - Many, many more...



Digital Identity Usage

- Digital identity credentials must satisfy two basic requirements
 - The credential being presented can be validated as coming from its stated source
 - The information “digitally signed” using the credential has not been modified from its original form



DI – Current Issues

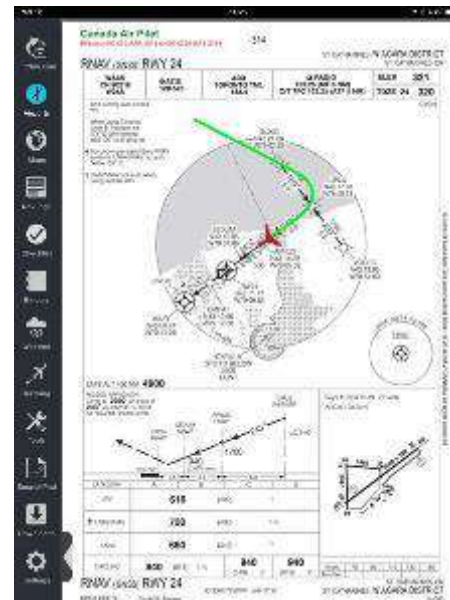
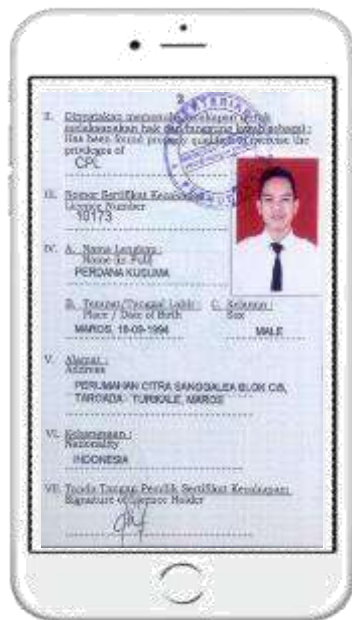
- Absent a global mechanism, digital credentials from different entities are not interoperable with each other
- Each entity issuing digital identities can choose its own implementation path and what information to include in its credentials
 - Lack of universally harmonized digital identity credentials format/content for civil aviation
 - Each data field in the digital credential can vary between entities (Boeing-777 ≠ Boeing 777)
- Inconsistent implementation of existing technical requirements
 - Where standards exist, there is no global policy to enforce them uniformly and consistently
- Lack of harmonized identity/credential assurance criteria between entities
 - A “highly” trusted credential in one context may not be trusted in another



ICAO

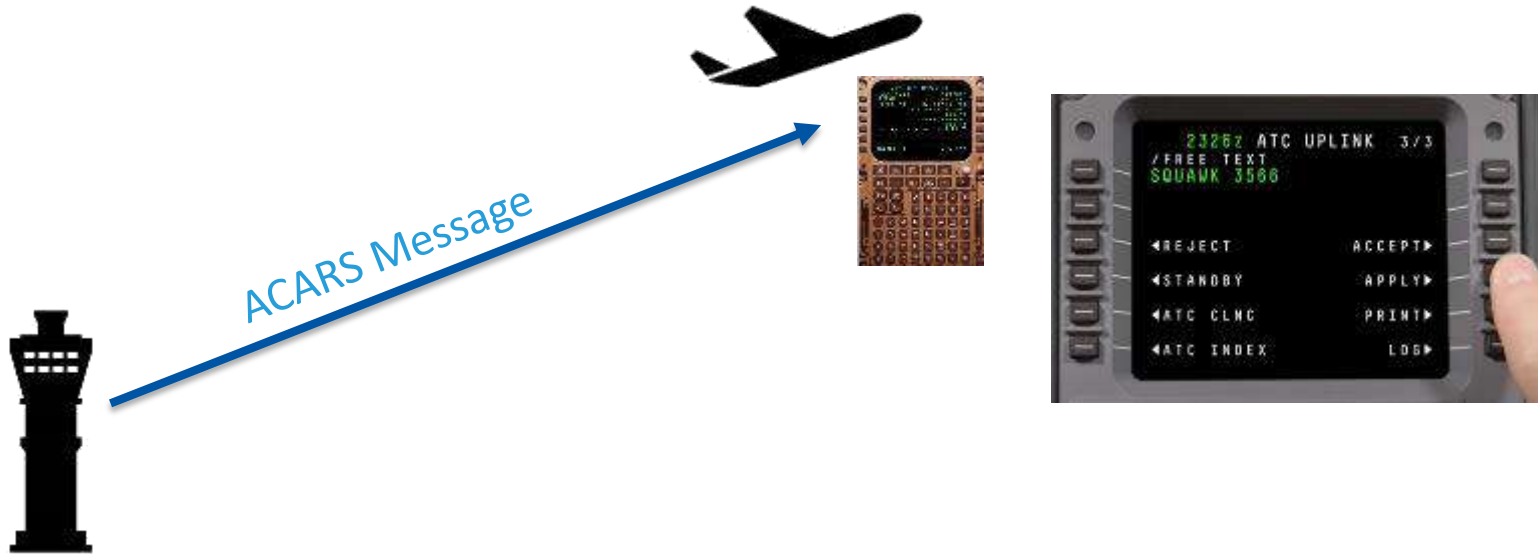
UNITING AVIATION

Are these valid?





Hypothetical Example

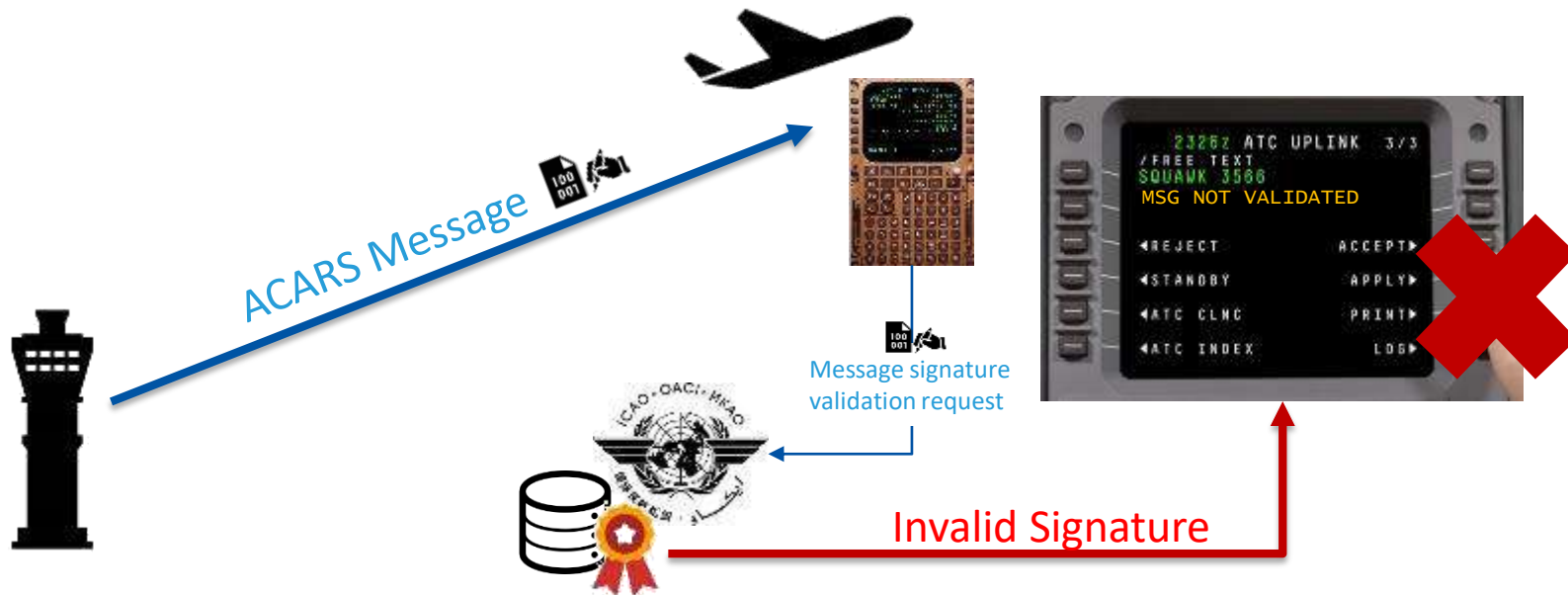




ICAO

UNITING AVIATION

Hypothetical Example





Digital Identity Pillars

- Digital Identity enables interoperability & trust via four pillars:
 - Legal framework
 - Global basis for mutually recognizing credentials
 - Operations
 - Operational policies to enable mutual recognition of credentials
 - Technical requirements
 - Criteria that ensure interoperability of credentials
 - Oversight
 - Continuous monitoring and follow-up of credential issuers against legal and policy requirements



DI – Implementation Considerations

- Adoption of operational and technical policies and technical requirements
- Identity credential cross-recognition mechanism requirements
- Business process speed differences between aviation stakeholders (airframers vs drones)
- Consideration of legacy systems (forward-fit vs. retrofit)

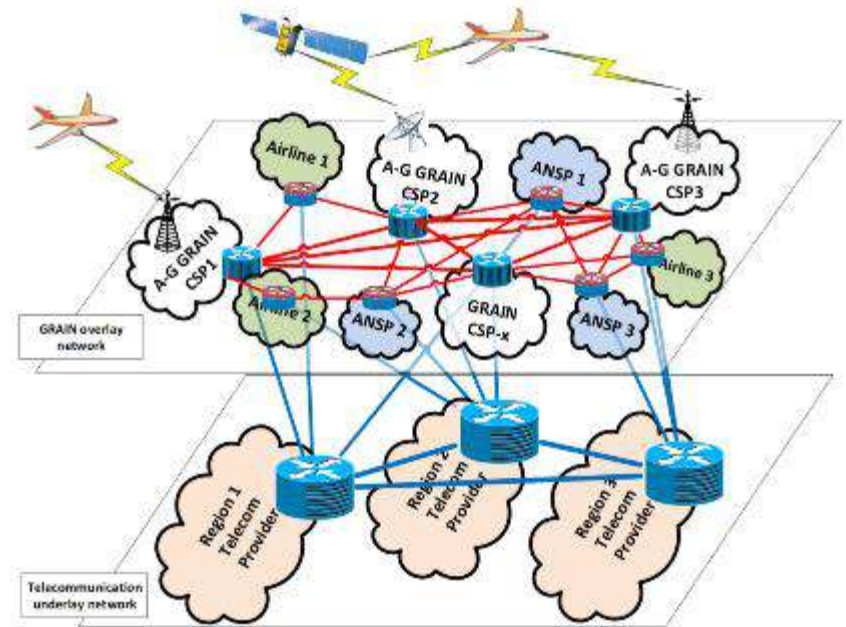


DI – The Future

- Digital credentials from different entities are interoperable with each other through a global mechanism
- Standardized digital credential structures, formats and contents
 - Universally harmonized digital identity credentials format/content for civil aviation applications
 - Credential data fields based on ICAO-standard values (e.g. Doc 8643)
- DI technical standards applied consistently across aviation stakeholders
 - Even stakeholders not participating in the trust framework will base their digital credentials on ICAO requirements to ensure forward-fit compatibility
- Globally harmonized identity/credential assurance criteria between entities
 - Robust and proven assurance mappings widely available

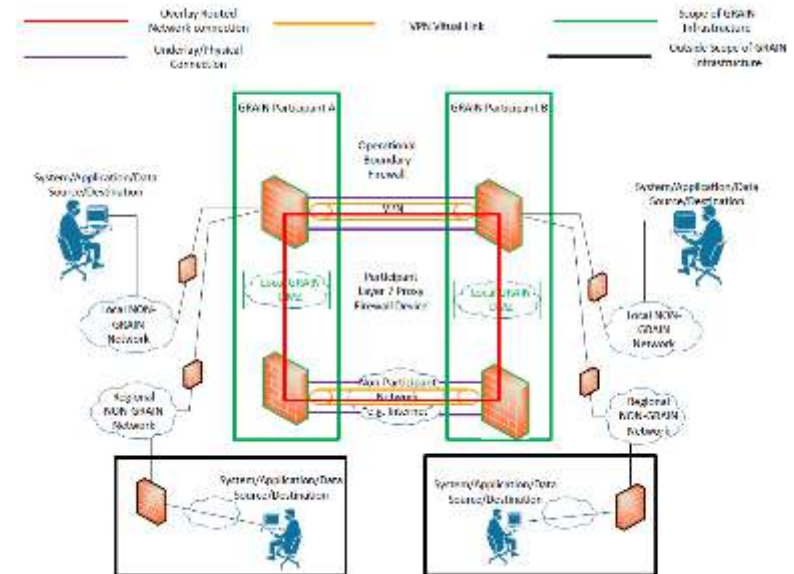
Network

- Virtual global network to connect regional and local aviation networks in a secure manner and provide for the necessary performance in the aviation system.



Network

- Technical requirements
 - IPv6 dedicated block
 - Domain Name System service requirements
 - Information security requirements
 - Network management requirements
 - Contingency plan requirements





Example IPv6 dedicated block

- Need for a dedicated IPv6 address block
 - Technical reasons (e.g. routing tables, SWIM)
 - Security layer (e.g. filtering)
 - Global recognition (e.g. allow aviation traffic)
- Develop a draft policy for the initial allocation and assignment of IPv6 addresses

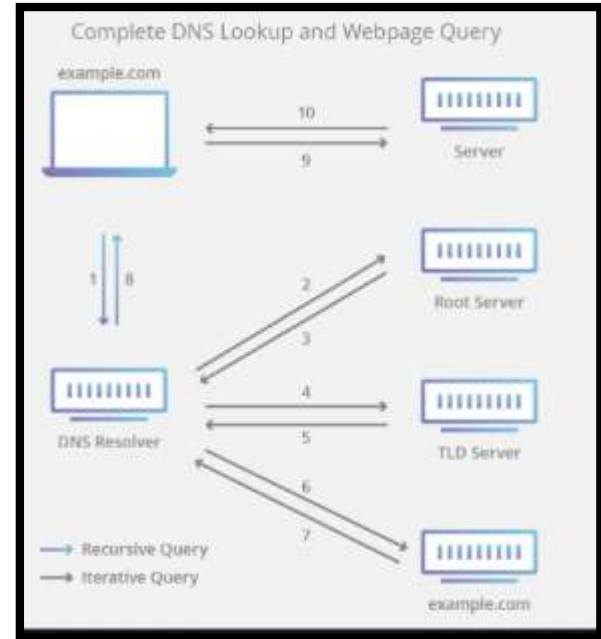
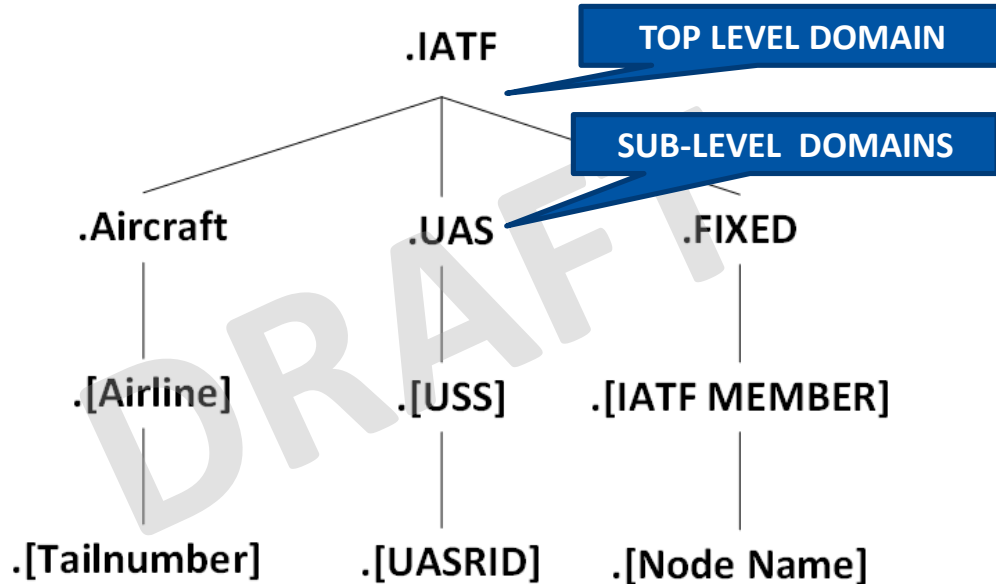


Example IPv6 dedicated block

/16 IANA Prefix Addressing Scheme of the largest estimated platform type

Bit #	Field Length	Purpose
1 – 16	16	ICAO IPv6 prefix
17 – 20	4	Platform type
21 – 28	8	States
29 – 38	10	USS per State (1024)
39 – 60	22	UAS per USS (4,000,000)
61 – 64	4	Subnets per UAS
65 – 128	64	Interface ID (per RFC 8064)

Example Domain Name System Service



Example Information Security requirement

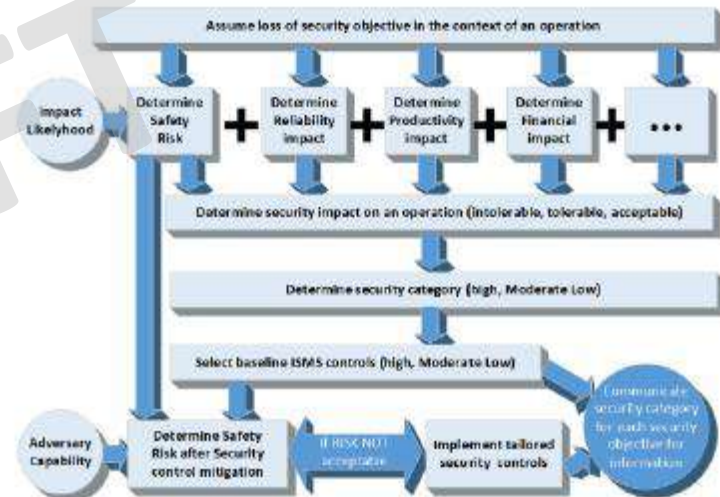
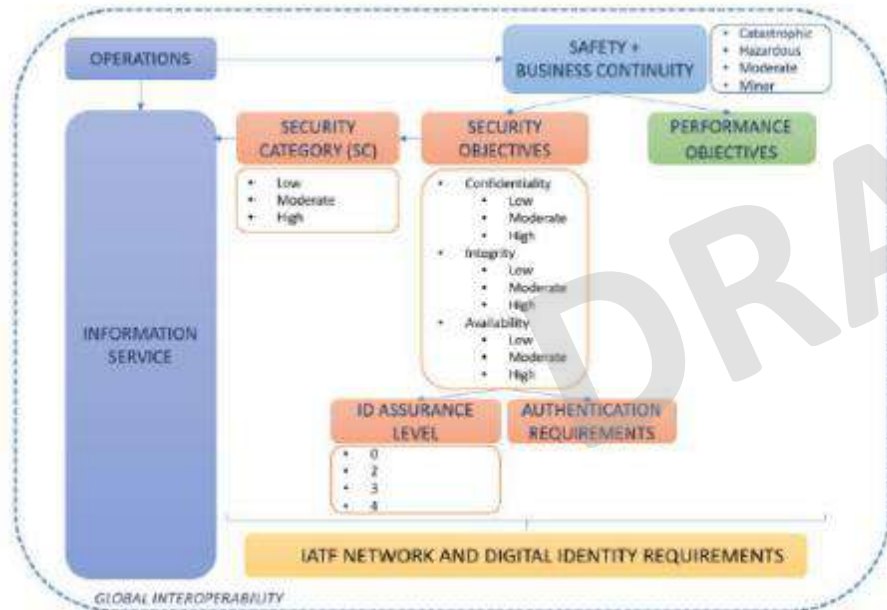


Figure 1 Process to determine the security category for information security objectives

Example Information Security requirement

Safety Risk Analysis (SRA) Risk Chart					
Minimum Capability Level	Novice/intermediate				
	Proficient				
	Organized				
	Integrated				
	Institutionalized				
Total Risks:		Minor	Major	Hazardous	Catastrophic
		Safety Impact			
Safety Risk Level	Recommended action				
INTOLERABLE	Take immediate action to mitigate the risk. Perform risk mitigation to ensure that additional or enhanced preventative controls are in place to bring down the safety risk level				
TOLERABLE	Can be tolerated based on the security risk mitigation. It may require management decision to accept the risk				
ACCEPTABLE	Acceptable as is. No further risk mitigation required				

Figure 4 Information security safety risk analysis chart

SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. SC sensor data = {(confidentiality, NA), (integrity, HIGH), (availability, HIGH)}, and SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.



Example Information Security requirement

ID	Objective	Description	Type O= Organization T= Technical	Performance			Security Triad		
				LOW	MEDIUM	HIGH	C	I	A
3.0	System Configuration and Management								
3.10	Information Protection At-Rest	The entity shall implement cryptographic mechanisms to protect information at-rest		Systems shall protect information stored on hard disks with a minimum security strength of 128 bit. <i>Note: confidentiality protection means encryption</i>	Systems shall protect information stored on hard disks with a minimum security strength of 192 bit. <i>Note: protection of information</i>	Systems shall protect information stored on hard disks with a minimum security strength of 256 bit.	X	X	
						Control Mapping			
						NIST 800-53	ISO 27001	ISO 27701	IATF C
						SC-28			

Control Mapping

NIST 800-53

ISO 27001

ISO 27701

IATF CP

SC-28

Example Network management requirements

- Monitoring of
 - Intrusion events
 - Security incident events
 - DDoS events
 - Anomalous traffic events
 - Outage events
 - Interface performance events
- Reporting of events



Figure 1 Shared Risk between Interconnected Aviation Stakeholders



Operations

- Management and allocation of IPv6 addresses
- Management of the domain name system service
- Run of the interoperability solutions lab
- Network monitoring
- Implementation of contingency plans



Oversight

- Auditors training and certification
- Auditing requirements
- Validation (independent validation? Self-validation?)
- Auditing escalation
- Audit report approval



CONCLUSION

- Trusted exchange of information is key to the future of the air navigation system
 - CNS/ATM systems and infrastructure must be ready to support trusted exchanges
- A global solution is necessary to enable universally accepted digital identities and end-to-end information security



ICAO

UNITING AVIATION



ICAO

North American
Central American
and Caribbean
(NACC) Office
Mexico City

South American
(SAM) Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
(WACAF) Office
Dakar

European and
North Atlantic
(EUR/NAT) Office
Paris

Middle East
(MID) Office
Cairo

Eastern and
Southern African
(ESAF) Office
Nairobi

Asia and Pacific
(APAC) Sub-office
Beijing

Asia and Pacific
(APAC) Office
Bangkok

THANK YOU

 Q&A

SP101 – ICAO Trust Framework Latest Development

14 Jun 2021, 08:00 - 16:00

by Ms. Olga De Frutos Martin and Mr. Michael Goodfellow Technical Officers, Air Navigation Capacity and Efficiency (AN), Air Navigation Bureau, International Civil Aviation Organization (ICAO)

72 Participants 48 Interactions*	38 Total votes 8 Highest vote	9 Questions 9 Allowed 0 Dismissed	3 Questions answered
--	---	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

9 Questions Allowed

8
VOTES

Anonymous • 14 Jun 2021 08:52 • ✓ ANSWERED

How do IATF affect the APACs decision to implement SWIM registry implementation?

7
VOTES

Anonymous • 14 Jun 2021 08:26 • ✓ ANSWERED

Do there any examples of IATF that are already operating in place? How APAC can share their experience in implementation?

1 Comment:

Zaki (CAA Singapore) • Allowed on 14 Jun 2021, 08:27 • Shown

I do not think so, still works in progress right?

0 Upvotes | 0 Downvotes

6
VOTES

Anonymous • 14 Jun 2021 08:23 • ✓ ANSWERED

How the IATF to incorporated into the existing projects currently proceeding in APAC - eg CRV and SWIM?

5
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 08:42

There was discussion of using IPv6 before when implementing AMHS in the APAC, but it was dropped, how will it be implemented again in the CRV?

4
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 08:57

I understand that is such audit for USOAP audit for ANS. Will the audit be under the USOAP?

3
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 08:26

Is this concept similar to the COVID-19 vaccination digital passport, where all international airport will recognize the digital passport, being verified and authenticated

2
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 08:55

For CRV, there is Operational Group (OG) for the APAC region to maintain and meet to discuss technical issues, will there be another group for running and maintaining this IATF?

2
VOTES

Baogang Chen(atmb,CAAC) • 14 Jun 2021 09:03

Identity authentication is certainly effective for gentlemen or insiders, but for hackers or external network security threats, identity authentication is often bypassed. How to consider?

1
VOTE

Anonymous • 14 Jun 2021 08:42

You mentioned about UTM RPAS and ETM. How IATF to regulate / operate in these area?



Importance of IATF to FAA

Rob Segers NAS ISS Architect

June 2021



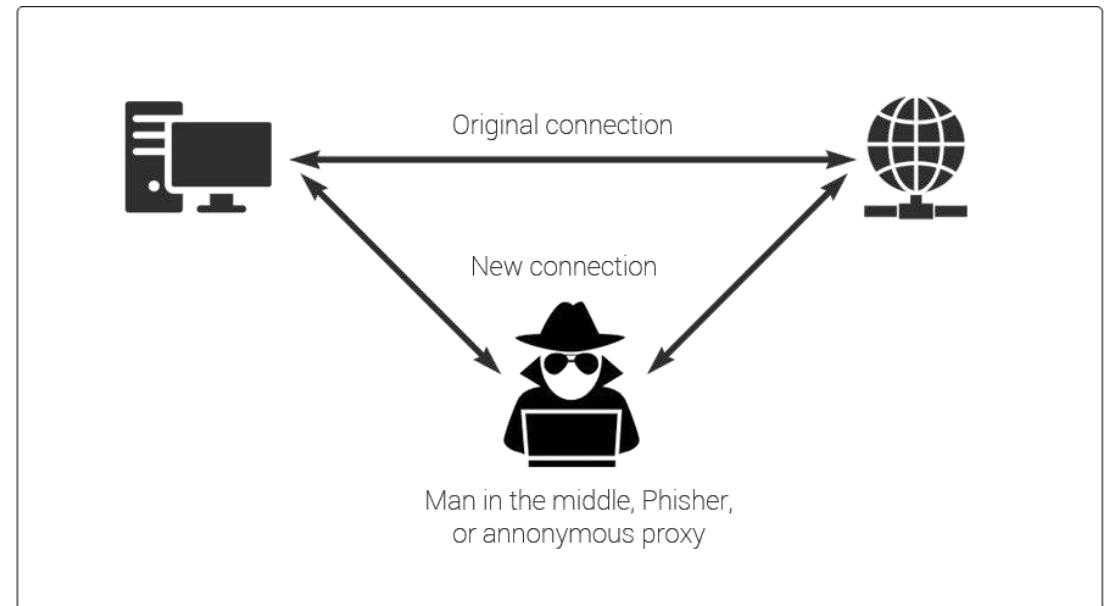
Problem Statement

- The cost of fit for purpose networks and the use of protected spectrum limits the ability to grow the network connectivity, bandwidth and worldwide ATM automation integration required to grow aviation capacity and the integration of Unmanned Aircraft Systems
- The use of ubiquitous network peering across commercial networks including unprotected spectrum will require end to end information integrity between information producer and consumer to assure network trust and safety



Man in the Middle (MITM) Attacks: an Aviation Threat

- Man-in-the-middle(MITM) attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation
- The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected party
- A MITM attack allows the attacker to eavesdrop on the conversation between the parties, or to actively intervene in the conversation to achieve some illegitimate end



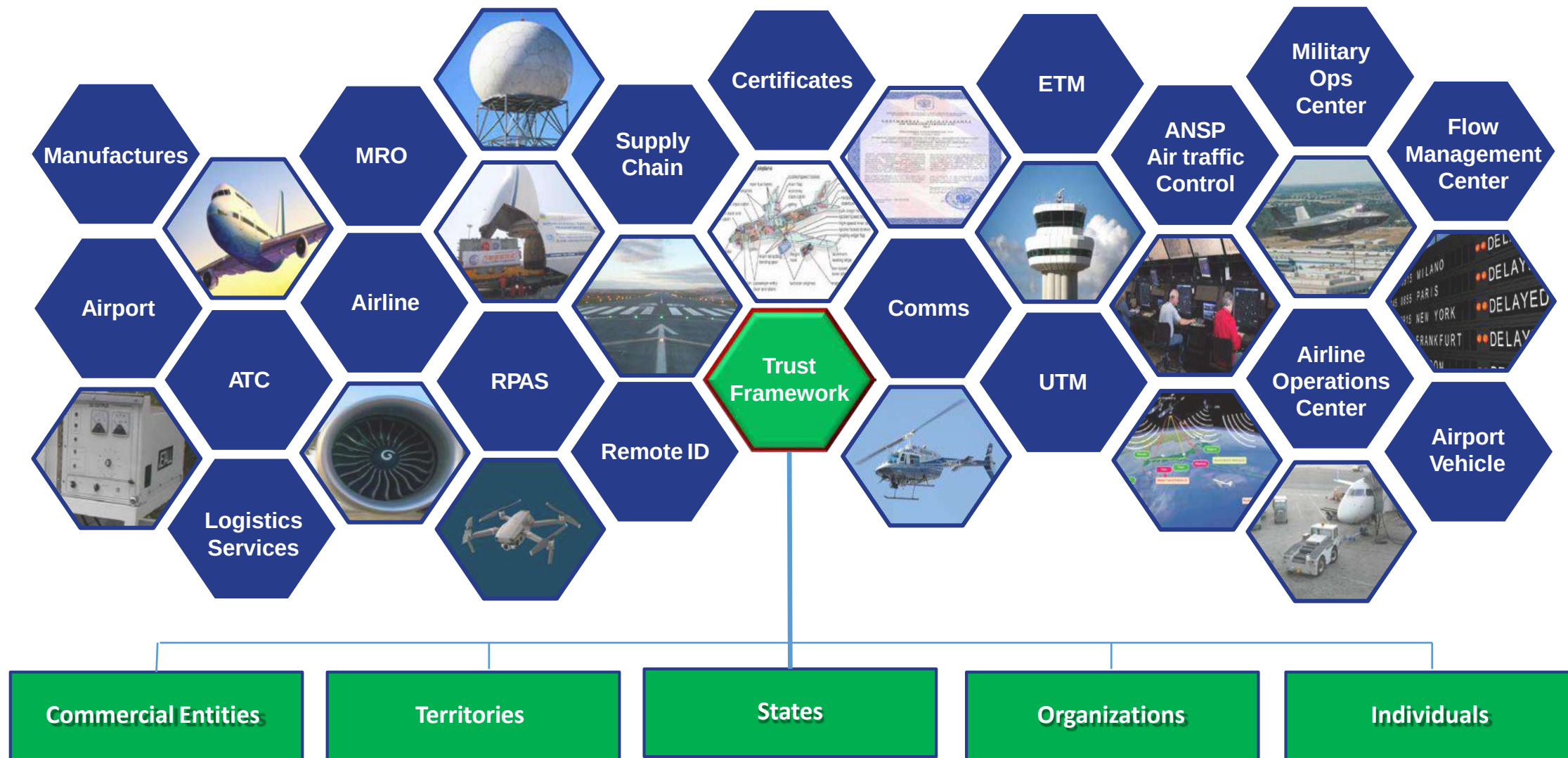
- A MITM attack can also occur by modifying information at rest (e.g. stored on a cloud server)

Problem Statement (continued)

- Current compliance to standards and regulations does not provide identity and information security interoperability
- As a result of the lack of information security interoperability, there is no guarantee of end to end information protection
- Regulatory oversight (e.g. Hierarchical compliance verification) through ICAO auditing regulators and regulators auditing service providers does not provide security interoperability
- Information security interoperability (Trust) is currently established organization by organization and on a project by project basis
 - not scalable
 - complex
 - costly
 - increase of attack surface
 - lack of harmonization undermines confidence in information protection



Common Need Across the Ecosystem... Establish Trust and Resiliency



Operationalization of the Trust Framework

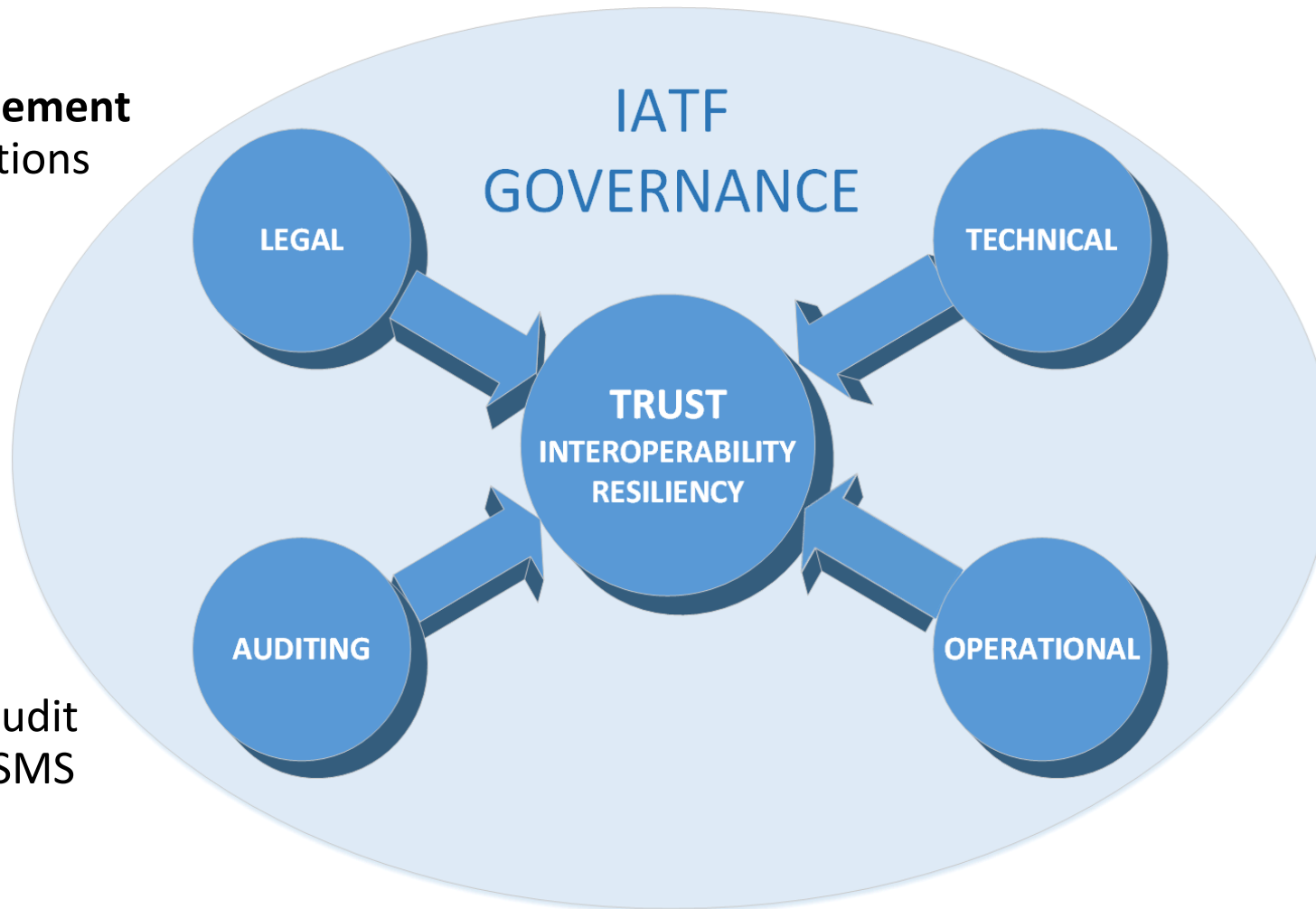
International Aviation Trust Framework (IATF)

- **Unified legal agreement**

- Terms and conditions
- Liabilities
- Indemnifications
- Warranties

- **Industry based audit practice**

- e.g. Web trust Audit
- e.g. ISO 27001 ISMS



- **Managed performance based requirements**

- Trusted Identities
 - Identity policy
- Trusted Networks
 - Network policy

- **Managed services**

- Trust Anchor
- Domain Naming
- Network addressing
- Security Monitoring
- Interoperability Lab

Importance of IATF to FAA



- North American Interactions between FAA and Nav Canada for Canadian international flights.
- North American Interactions between FAA within Services a la Navegacion en el Espacio Aereo Mexicano (SENEAM) in Mexico.
- Transition to IP networks and SWIM.
- Need for Federated Identity and Access Rights to secure internal FAA and international transactions

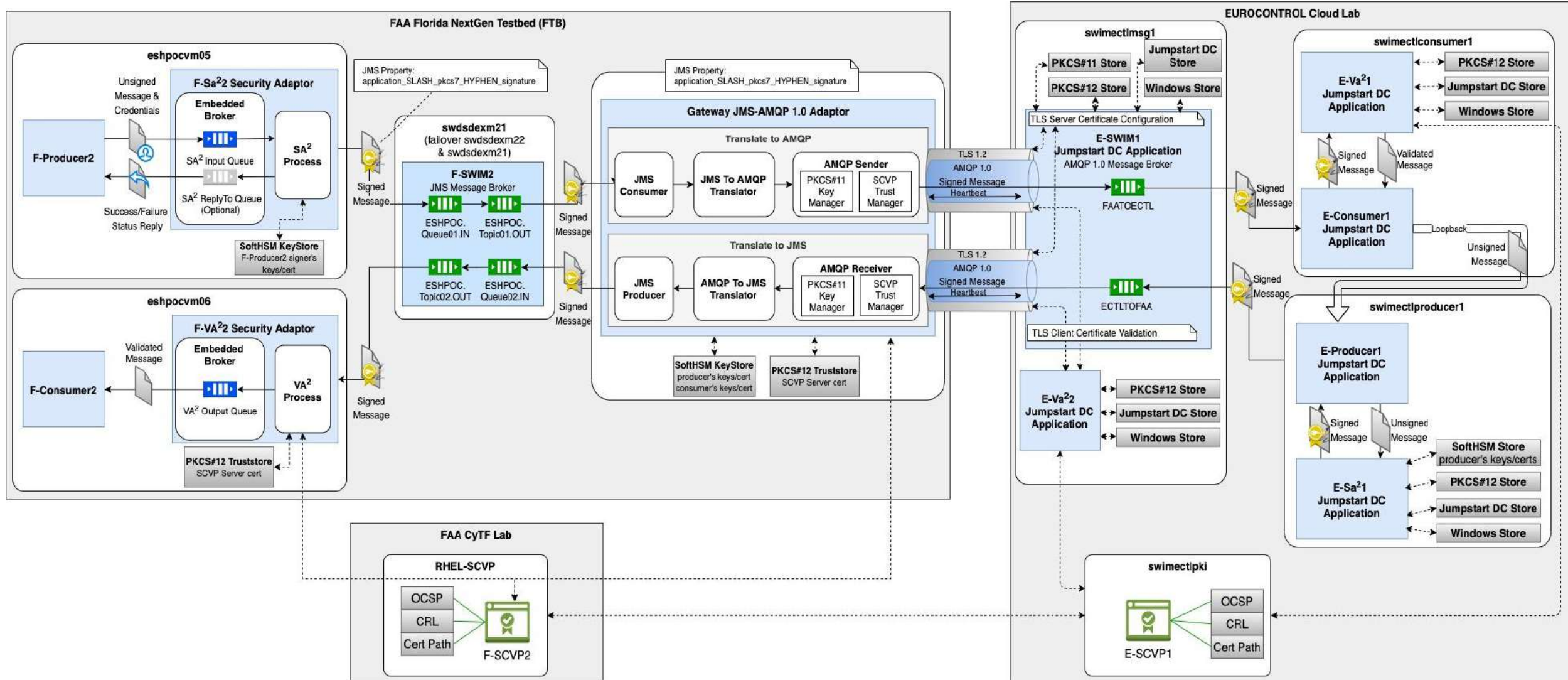
Enterprise Security Harmonization Proof Of Concept

Testing the IATF Identity management approach

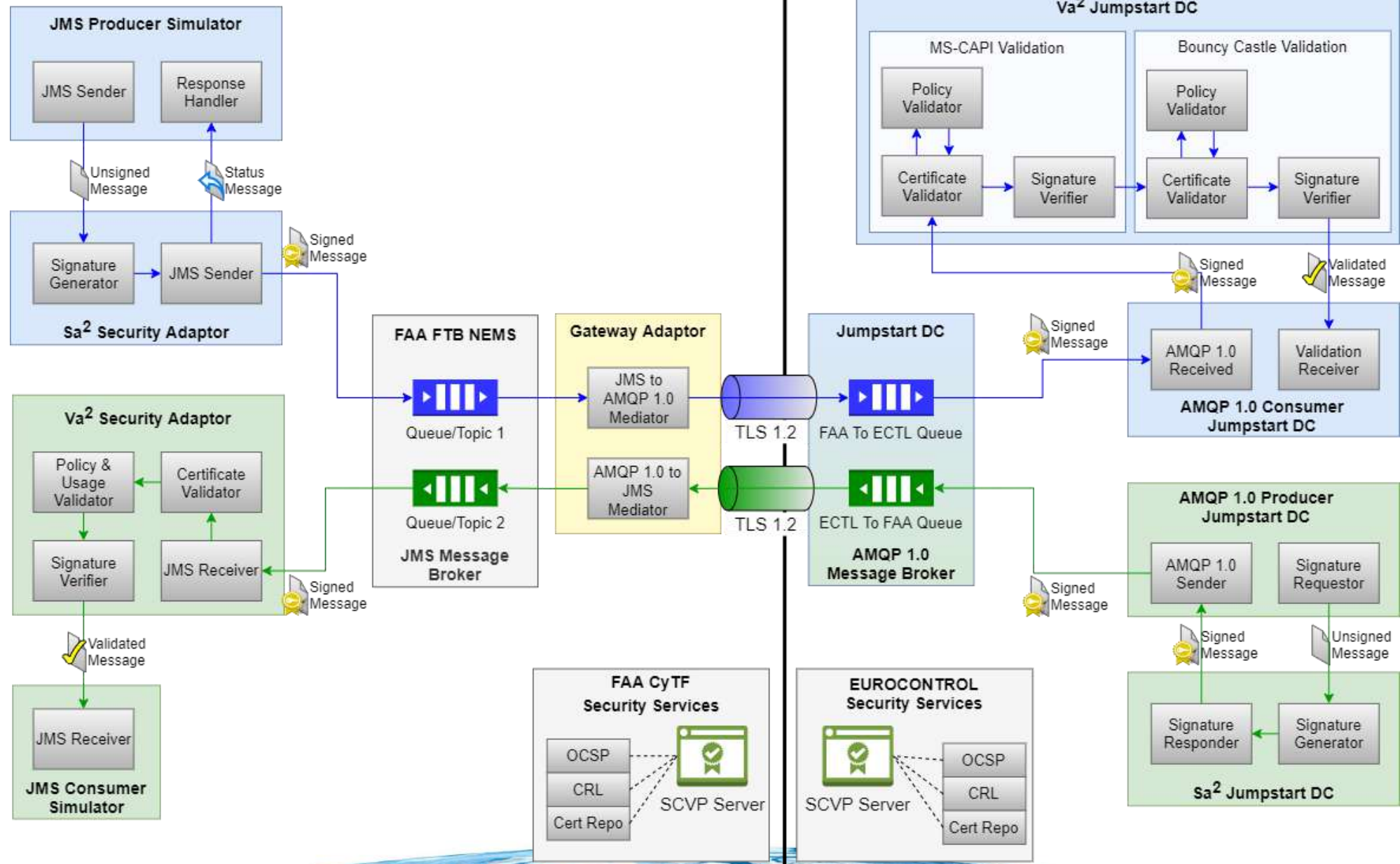
- The Enterprise Security Harmonization Proof Of Concept (ESHPOC) was started as part of the Coordination Plan (CP) 1.8 Enterprise Security between FAA NextGen and EU SESAR with as goal to
 - Harmonize enterprise security between NextGen and SESAR
 - Establish a proof of concept of the Trust Framework Study Group (TFSG) identity management approach between Europe and the US
 - Show security interoperability between Europe and the US SWIM leveraging multiple Public key Infrastructure (PKI) methods to establish trust
- The TFSG has harmonized the International Aviation Trust Framework (IATF) PKI Certificate Policy (CP) used for ESHPOC



Detailed ESHPOC System Architecture

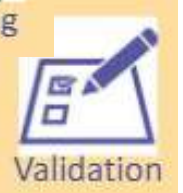


Simplified System Architecture



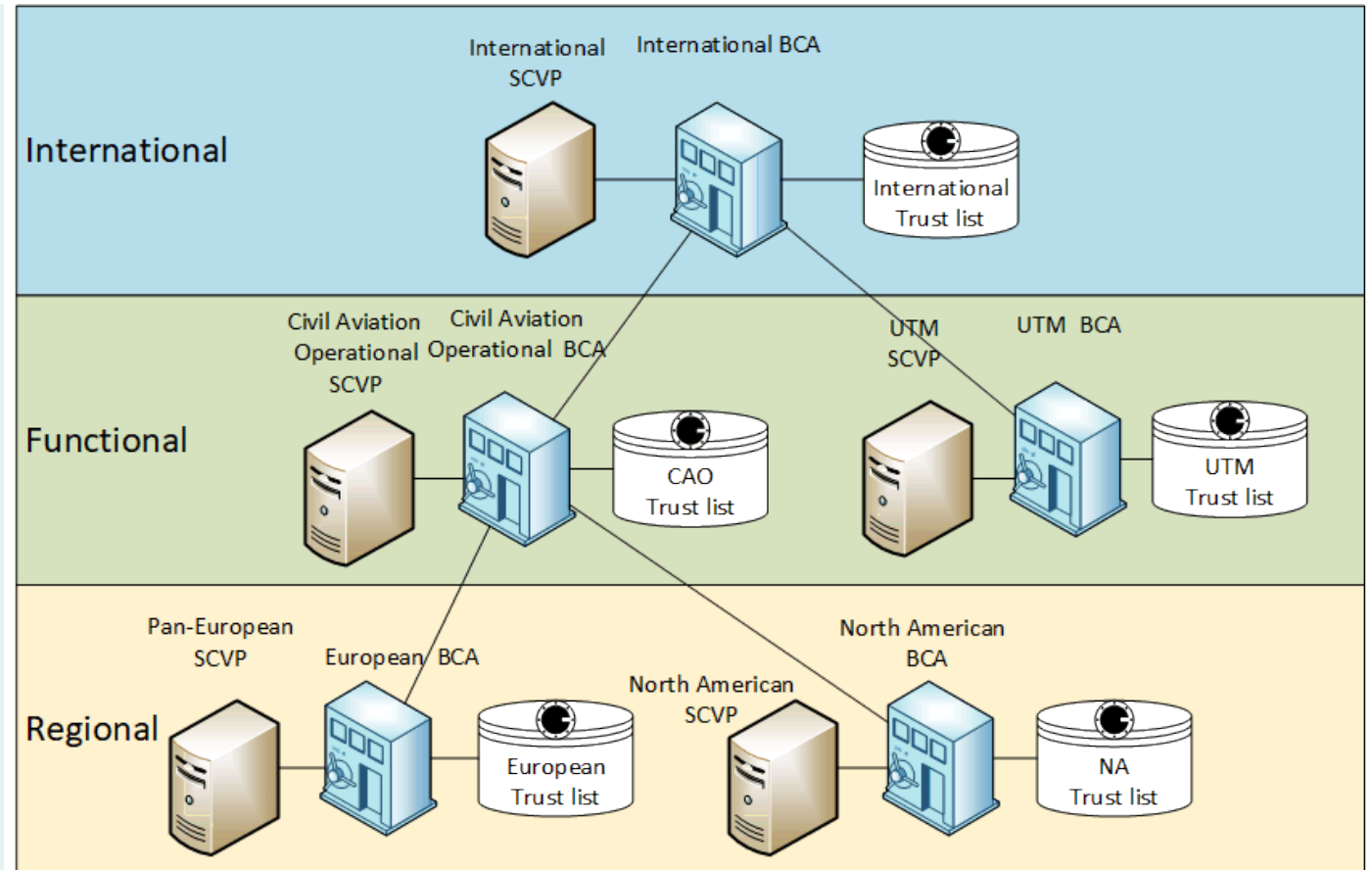
ESHPOC Main achievements - Security Interoperability

- ✓ **Integrity protected SWIM** messages can now be mediated between Java Message Service [FAA] and Advanced Message Queuing Protocol (AMQP) 1.0 [EU] implementations
- ✓ **Signing as a Service (Sa2)** and **Validation as a Service (Va2)** in the context of SWIM message exchange between international organizations is now feasible
- ✓ **Sa2 and Va2 are backwards compatible** and allow organizations to implement independently
- ✓ **Validation of fit** for purpose SWIM Public Key Infrastructure (PKI) certificates using SWIM specific policies is now feasible



ESHPOC Main achievements (continued)

Trust between international CA's through the use of a **Bridge Certificate Authority (BCA)** and **Certificate Trust List (CTL)** can be established and should be used at the international, functional and regional level.



Hierarchy allows scaling and scope management

ESHPOC Gap analysis - Findings

- To ensure **interoperability**, the use of CTL requires the development and adoption of a standardized CTL schema that is fit for aviation purposes.
- SCVP COTS vendors should implement **blacklisting and validation of certificates** with multiple policies
- Some COTS certificate validation products are **not compliant with RFC 5055 SCVP** and have limitations
- Certificate validation boundary cases demonstrate potential **trade-offs between safety and security**



ESHPOC Gap analysis - Recommendations

- Develop a **Specification for mediation** between AMQP 1.0 and JMS
- **Cryptographic Message Syntax (CMS)** used to handle end to end message level security CMS has proven its efficiency and robustness and a standard CMS profile should be adopted
- The study of and **standardization of international federated tokens** is recommended as a follow-up project in particular to address scalability issues raised by Multiple Certificate Policy identifiers



Future FAA needs for IATF Alignment

- Operate an enterprise wide PKI using a certificate policy that meets the IATF requirements.
- Manage Digital Identities using an enterprise wide Policy Management Authority (PMA).
- Expand the use of federated identities to federate access for external users.
- Incorporate GRAIN requirements into SWIM and all external interfaces.
- Active participation in the operationalization and membership of the IATF



Questions?



 Q&A

SP102 – FAA’s contribution to the IATF and Importance of IATF to FAA

14 Jun 2021, 08:00 - 16:00

by Mr. Robert Segers NAS Information Systems Security Architect, Member of the ICAO Trust Framework Study Group, Federal Aviation Administration

56 Participants 63 Interactions*	45 Total votes 11 Highest vote	18 Questions 18 Allowed 0 Dismissed	3 Questions answered
--	--	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

18 Questions Allowed

11
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 09:14 • ✓ ANSWERED

Who is managing this PKI? Who is the Certification Authority (CA)?

6
VOTES

Anonymous • 14 Jun 2021 08:29 • ✓ ANSWERED

Why do we need an operational trust framework? Other aviation eco-system areas are implemented through state regulation and industry compliance. Why is this different?

4
VOTES

Anonymous • 14 Jun 2021 08:30

How do new entrants like Unmanned Aircraft Systems (UAS) and Unmanned Aircraft System Traffic Management (UTM) fit within the trust framework?

4
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 09:25 • ✓ ANSWERED

For the CMS, what is the strength of the key? 256-bit? RSA?

3
VOTES

Anonymous • 14 Jun 2021 08:29

What is the relation between the US federal bridge Public Key Infrastructure (PKI) policy and the International Aviation Trust Framework (IATF) certificate policy?

3
VOTES

Anonymous • 14 Jun 2021 08:32

How could AI help implementing and maintaining cyber resiliency?

2
VOTES

Anonymous • 14 Jun 2021 08:31

Can we implement trust without resorting to encryption? Could such a system be cyber resilient? Are reliability and resilience the same concepts?

2
VOTES

Anonymous • 14 Jun 2021 08:31

What measures is the Trust Framework Study Group (TFSG) taking to ensure robustness, resiliency and future proofing against technology changes?

1
VOTE

Anonymous • 14 Jun 2021 08:28

If IATF requires auditing, how do you ensure that its requirements don't conflict with ICAO or a national regulator?

1
VOTE

Anonymous • 14 Jun 2021 08:29

How do you ensure that the Public Key infrastructure is acceptable by all regions in the world?

1
VOTE

Anonymous • 14 Jun 2021 08:29

What are the biggest challenges to ensure success for implementing the trust framework?

1
VOTE

Anonymous • 14 Jun 2021 08:30

How can you ensure that the trust framework can handle the large number of different operational aspects of the aviation eco-system?

1
VOTE

Anonymous • 14 Jun 2021 08:30

What happens when a trust framework participant doesn't comply with the requirements?

1
VOTE

Anonymous • 14 Jun 2021 08:30

Is Global Resilience Aviation Interoperable Network (GRAIN) a single physical network like the internet?

1
VOTE

Anonymous • 14 Jun 2021 08:31

What is the relation between Global Resilience Aviation Interoperable Network (GRAIN) and the internet?

1
VOTE

Anonymous • 14 Jun 2021 08:31

What is the role of ICAO in the operation of the IATF?

1
VOTE

Anonymous • 14 Jun 2021 08:32

Is ATM/UTM integration speeding up resilience efforts?

1
VOTE

Anonymous • 14 Jun 2021 08:33

Why do we need GRAIN? We have AFTN & AHMS today and Europe and Asia have implemented their own regional networks.

CANSO Standard of Excellence in Cyber Security



ICAO Asia/Pacific Regional Cybersecurity Webinar – June 2021



Shayne Campbell
Safety Programme Manager
CANSO



Have we just been lucky so far...?

There have been security incidents that have affected aviation, but no truly disruptive cyber event.

Is that because we're "good", or because we've been "lucky"?

⇒ The "Good"

- We have a culture of care and attention to support safety
- Our systems generally operate in an isolated environment (but this is changing...)
- Our processes and procedures are naturally defensive & cautious
- We have checklists of checklists

⇒ What if...

- ... our safety focus can be used to distract from other threats?
- ... the systems we trust implicitly have been altered?
- ... our caution stops us acting quickly when we need to?
- ... our checklists & procedures make us predictable to an attacker?
- ... a supplier we trust gets compromised?



CASE STUDY: SolarWinds "SUNBURST" Attack

Probably the most publicised attack so far in 2021

In late 2020, SolarWinds discovered malicious code had been inserted into its Orion monitoring product.

The malicious code was distributed to customers around March 2020.

The attackers first accessed internal SolarWinds systems in Sept 2019.

*Information taken from Microsoft Security's
Deep Dive into Solorigate/SUNBURST^[1]*



Step 1 – Unauthorised Access

The attackers covertly found a way into SolarWinds' systems and established a persistent capability.



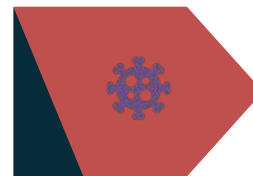
Step 2 - Research

The attackers spent time researching the protections SolarWinds had in place and finding a way to use them maliciously.



Step 3 - Deployment

The attackers deployed 4,000 lines of malicious code, packaged as a genuine part of Orion



Step 4 - Compromise

The code was designed to provide an entry point into end user organisations.

Even in isolated environments.



[1] <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>

Establishing Cyber 'Policy' is a great place to start

But isn't security about technical protections, firewalls and keeping 10,000 unique passwords?

These technical protections need to build on a solid foundation:

Risk Management

Business is about **managing risk**, so this is about managing security in a way that is familiar and well understood.



Regulation

Aka **Governance** – independent oversight to help keep the right behaviours happening.



Maintenance

Protecting against **supply chain** attacks via maintenance partners



Comms Security

Protecting against **impersonation** and **being influenced** by anonymous attackers



Handling Incidents

Consider an incident might be an **intelligent attacker** rather than a statistical event.

Think about **Business Continuity**, maybe graceful degradation of service.

Also consider **Disaster Recovery** – how to rebuild from nothing.

Share knowledge and **work together** - even commercial competitors are on the same side against attackers.



New Systems

Design in **foundational security**, and make sure **procurement chains** are trustworthy and not compromised



Access Control

Both **physical** and **logical**, use of least privilege, etc.



Ops Security

Building good cyber into operational processes



Asset Management

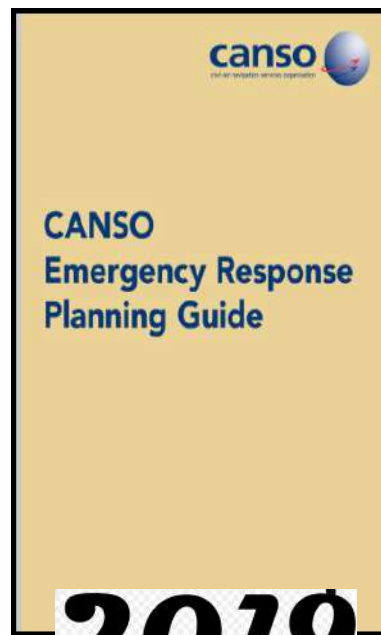
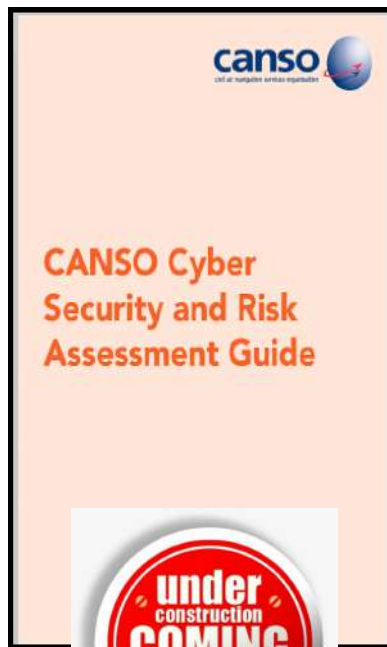
Knowing what you have, and what vulnerabilities you might be exposed to



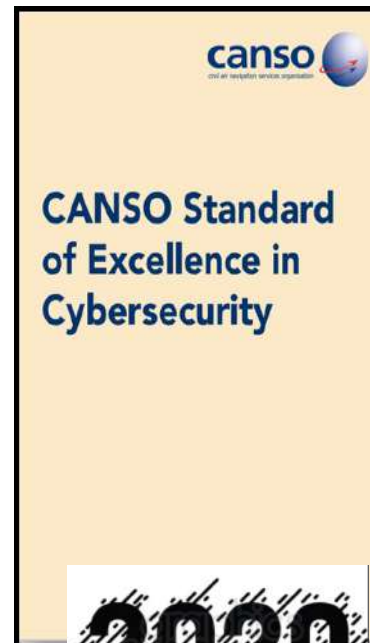
Policy stands as the foundation of good technical protections



CANSO Cyber Toolkit



2019



2020



2020



<https://canso.org/publications/>

SoE Maturity Levels



Example: Information Sharing

Where are we currently?

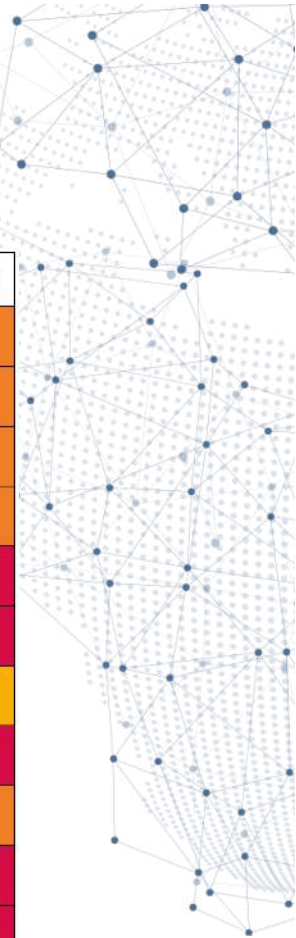
Maturity levels						
Element	Description	A Informal Arrangements	B Defined	C Managed	D Assured	E Optimised
Information sharing	The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties	No, or very limited, cybersecurity information sharing	Using some threat intelligence and vulnerability information; Informal information sharing internally and externally where appropriate	Trends are identified; Internal and external sharing based on formal processes linked to risk assessment, vulnerability management, response and recovery processes; Relevant risk information is shared between safety and security functions	Threat intelligence and vulnerability information for all critical systems; Consistent, widespread and effective sharing between all relevant parties.	Information sharing is habitual and proactive; demonstrable leadership in improving industry-wide information sharing

Assessment is supported by probing questions for ANSPs and suppliers
SoE contains loads of advice and lessons learned



Example Assessment Results

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Identity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B



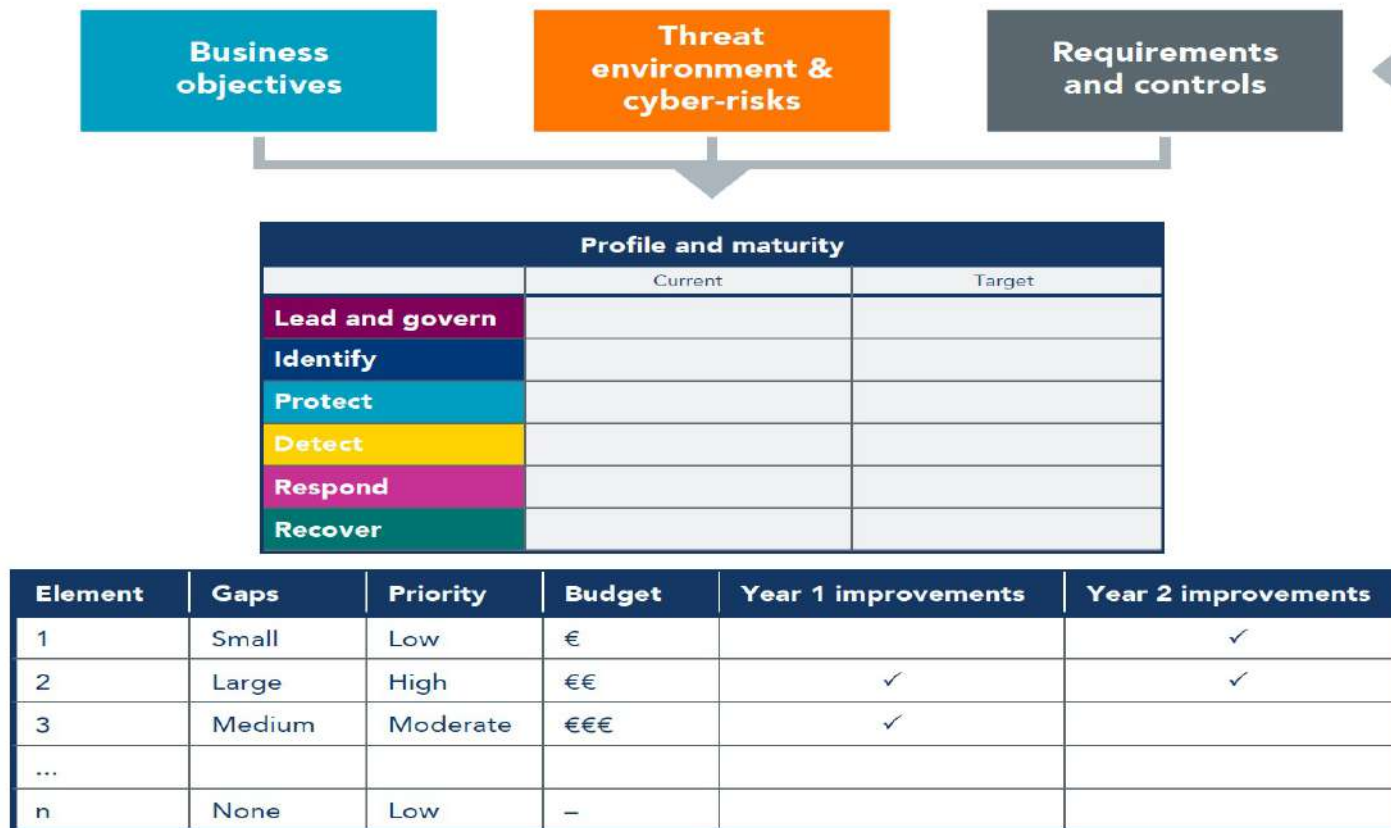
YAMM 🧐

Yet Another Maturity Model???

Yes, but

- it is *aimed at ATM* – so it is relevant for us (at least for many of us in ATC...)
- it aims to focus on security *in a safety-related context*
- it has already been and will likely be *used by our customers* to assess us
- it is very simple and a *self-assessment* should be possible in *less than a day!*

What to do with the results of the SoE?





Visit us:
canso.org



 Q&A

SP103 – Cyber Safety in ATM

14 Jun 2021, 08:00 - 16:00

by Mr. Shayne Campbell Safety Programme Manager, CANSO

60 Participants 33 Interactions*	21 Total votes 7 Highest vote	7 Questions 7 Allowed 0 Dismissed	7 Questions answered
--	---	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

7 Questions Allowed

7
VOTES

Anonymous • 14 Jun 2021 08:41 • ✓ ANSWERED

CANSO has provided a very comprehensive SoE for ANSPs/CAAs to follow. With all the ISO270xx/NIST/ICAO Docs, how this SoE are expected to be employed?

1 Answer:



Admin

Submitted on 15 Jun 2021, 13:40

(Transcript from Webinar) This is a conversation that we have had many many times. SoE is agnostic to what type of standard you are following. If you really look at it and if you are following the NIST directive, then you should be able to apply the model, the SoE, based on the requirement in the NIST. The conversations have happened at many different levels and in many different times – one of the things that have come through is that it does not matter what standards of you are following, this (SoE) will apply to any standards.

5
VOTES

India Senthilvel Balasubramanian • 14 Jun 2021 10:14 • ✓ ANSWERED

Do we have any measured maturity levels of cyber security of organizations those who have participated in making the CANSO cyber toolkit.

1 Answer:



Shayne Campbell, Safety Programme Manager

CANSO • Submitted on 15 Jun 2021, 11:33

Yes, we do. I do know there are ANSPs willing to share that information with other CANSO Members.

1 Comment:

Shayne Campbell • Allowed on 14 Jun 2021, 10:26 • Hidden

Yes, we do. I do know there are ANSPs willing to share that information with other CANSO Members.

0 Upvotes | 0 Downvotes

5
VOTES

India Senthilvel Balasubramanian • 14 Jun 2021 10:14 • ✓ ANSWERED

What are CANSO's inputs for preparing the competent human resources for making the aviation organization to achieve higher maturity levels.

1 Answer:



Admin

Submitted on 15 Jun 2021, 13:39

(Transcript from Webinar) The CANSO believes that cyber is a threat that is going to grow larger as we get into more complex systems. There has been ongoing conversations about "beefing up" the security profile inside your organization, meaning that as ANSPs have finite budget to work with, and ANSPs should find the appropriate resources needed to really equip the expertise needed for cyber. The good news is we (CANSO) have a lot of associate members within CANSO are cyber experts. I am not a cyber expert but I have worked with some top notch people. They helped me to prepare the presentation and gave me a lot of detail. CANSO have that access of these people come in and say this is what you need. Hence it does not always need to have internal solutions, sometimes there are good external solutions that can get organizations up to speed but this is a priority for CANSO members.

2
VOTES

Anonymous • 14 Jun 2021 10:18 • ✓ ANSWERED

On YAMM - so how CANSO expects CAAs to run this Standard of Excellent model on parallel with existing CAAs own framework and other models from ISO, ICAO Docs and NIST?

1 Answer:



Shayne Campbell, Safety Programme Manager

CANSO • Submitted on 15 Jun 2021, 11:33

The SoE was designed for ANSPs to utilize. Much like other SoEs, the results can be used to demonstrate to CAAs where they are along the path.

1 Comment:

Shayne Campbell • Allowed on 14 Jun 2021, 10:28 • Hidden

The SoE was designed for ANSPs to utilize. Much like other SoEs, the results can be used to demonstrate to CAAs where they are along the path.

0 Upvotes | 0 Downvotes

1
VOTE

Anonymous • 14 Jun 2021 10:17 • ✓ ANSWERED

How does CANSO SoE Maturity Model relate to other organisational maturity models? Is it readily mappable in terms of maturity levels?

1 Answer:



Shayne Campbell, Safety Programme Manager

CANSO • Submitted on 15 Jun 2021, 11:32

Yes, it certainly is. All CANSO SoE's have five levels of maturity and can easily be mapped to other maturity models.

1 Comment:

Shayne Campbell • Allowed on 14 Jun 2021, 10:29 • Hidden

Yes, it certainly is. All CANSO SoE's have five levels of maturity and can easily be mapped to other maturity models.

0 Upvotes | 0 Downvotes

1
VOTE

Anonymous • 14 Jun 2021 10:20 • ✓ ANSWERED

What are the Specific Cyber Security Policies mandatorily to be implemented to secure CNS/ATM System in accordance with the applicable ICAO regulations by a state

1 Answer:



Shayne Campbell, Safety Programme Manager

CANSO • Submitted on 15 Jun 2021, 11:33

This is a great question and one for ICAO to elaborate on.

1 Comment:

Shayne Campbell • Allowed on 14 Jun 2021, 10:28 • Hidden

This is a great question and one for ICAO to elaborate on.

0 Upvotes | 0 Downvotes

0
VOTES

Anonymous • 14 Jun 2021 08:53 • ✓ ANSWERED

How well does this SoE be referenced and used in APAC State?

1 Answer:



Shayne Campbell, Safety Programme Manager

CANSO • Submitted on 15 Jun 2021, 11:39

The SoE is a very popular maturity model in the APAC region.

1 Comment:

Shayne Campbell • Allowed on 14 Jun 2021, 10:31 • Hidden

The SoE is a very popular maturity model in the APAC region.

0 Upvotes | 0 Downvotes

ICAO Asia & Pacific Regional Cybersecurity webinar

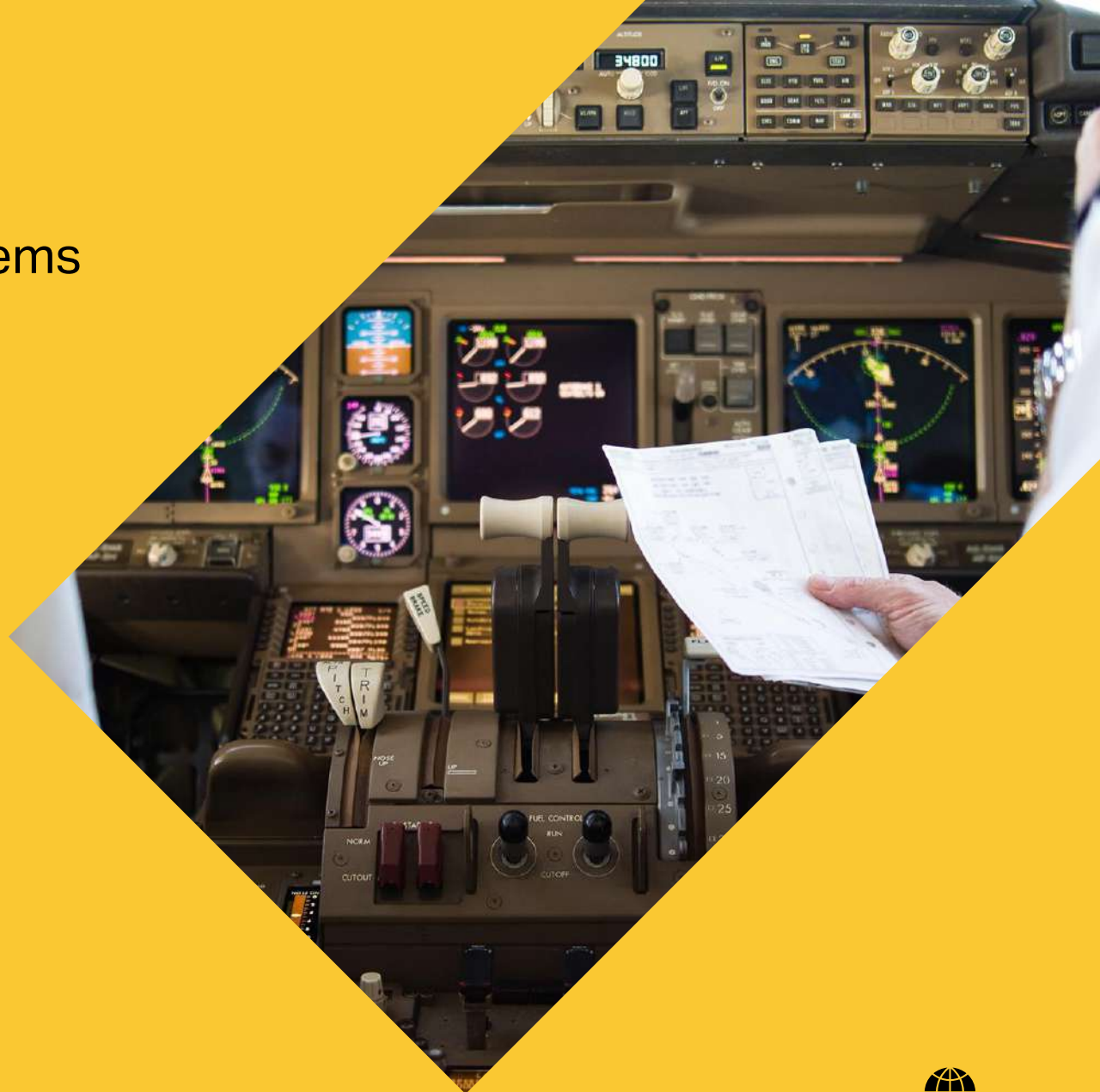
Management Framework for CNS/ATM Systems

Protecting All Systems

John Moore

Assistant Director,
Safety & Flight Operations
Asia-Pacific

14 June 2021



The Challenge



- Airlines have many business, financial and administrative systems
- Also, many Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) systems
- Solutions must protect all systems from cyber-attacks

Background

Increasing threat of cyber attacks in aviation

New generation aircraft are connecting to the ground in real-time

More networks, more digitization

Not just business systems – CNS/ATM as well

New entrants – UAS?

What needs to be done to ensure critical information & systems remain protected?



Today's protection?

Aviation security historically strong

Mature Governance

Critical systems and safety-critical information 'isolated'

Firewalls protect against penetration

Data and information via secure pathways, eg: CRV

Encryption

Current environment

- Many connections now and more foreseen
- Datalinks between aircraft and ATM systems
- Point-to-point sharing and tight coupling through defined interfaces
- Defined procedures and governance
- High physical security
- Already connected in several ways in the cabin



Emerging Environment

Airlines seek continual safety and efficiency benefits

Increased connectivity for entertainment and communication – passenger experience

System Wide Information Management (SWIM) is becoming a game-changer

Cockpit connected via IP?

Electronic Flight Bags (EFBs)

Greater sharing of information between ground stations

Potential for less 'isolation', increased scope for attacks

What sort of attacks?

1. Denial of Service – prevents access to a service or system

Cockpit systems

Airline flight planning systems

Airline ticketing systems

Satellite interruption

ATM systems (surveillance and FDP)

Ground station or pathway interruptions

What sort of attacks?



2. Compromising or corrupting the integrity of data and / or information

Value of information?

Partial – deleting or blocking delivery of required data

Delayed – data or information is delayed causing systems to miss critical decision-points

Inaccurate – information is intentionally incorrect creating false analyses outcomes

What are potential consequences?

Avionics fail or become inaccurate and unreliable

Aircraft operation compromised

Airline systems corrupted (Flight Planning / Ticketing)

ATM systems – safety compromised

One incident can escalate

Electronic Flight Bags (EFBs)

- EFBs now widely used
- Connectivity creating significant efficiencies
- No incidents in 170 million flights using EFBs
- Various levels of current protection:
 - Vendor included strategies
 - OEM & airline cooperation
 - Company policies for connecting



Unmanned Aerial Systems (UAS)

- Growing number of UAS
- New capabilities more system interconnections
- Protecting against intentional damage
- New risks and vulnerabilities
- Perpetrators difficult to identify
- Mitigating cyber risks is key to enabling UAS



Prevention:

Safety by design – firewalls, encryption, standards

Layered resilience – in SMS planning

AI detection systems in CNS/ATM, aircraft, airline and airport systems

Rapid response and recovery capabilities

Strong Governance

Training and education

Physical security

ICAO Global Resilient Aviation Network ConOps



Summary

- Operational systems as well as business systems
- Current protection is strong
- Growing reliance on connectivity and system-of-systems integration
- More data sharing (SWIM, EFBs)
- New entrants (UAS)
- Must continue to evolve to ensure all systems will be protected



QUESTIONS?

John Moore
Assistant Director,
Safety & Flight Operations
Asia-Pacific
moorej@iata.org



 Q&A

SP201 – Protecting All Systems

14 Jun 2021, 08:00 - 16:00

by Mr. John Moore Assistant Director, Safety and Flight Operations-ASPAC, International Air Transport Association (IATA)

51 Participants 42 Interactions*	36 Total votes 11 Highest vote	4 Questions 4 Allowed 0 Dismissed	4 Questions answered
--	--	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

4 Questions Allowed

11
VOTES

India • 14 Jun 2021 10:33 • ✓ ANSWERED

Are the Cyber Security Audits done by ICAO to ensure the applicable regulations implemented by a state to secure their CNS/ATM System.

9
VOTES

Anonymous • 14 Jun 2021 09:08 • ✓ ANSWERED

There are recent breach of pax info reported like SITA for StarAlliance and Air India. How IATA assists these companies in handling these threats?

1 Comment:

IND_CNS_SATYA • Allowed on 14 Jun 2021, 10:48 • Shown

There are lots of online data available in public domain, which adds more threat. How IATA plans to mitigate?

0 Upvotes | 0 Downvotes

9
VOTES

Anonymous • 14 Jun 2021 08:36 • ✓ ANSWERED

Do you think that due to the significant reduction in operations during the COVID-19 interruption that airlines have changed their priority for investing in cyber-security?

7
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 10:38 • ✓ ANSWERED

CRV goes to the layer 2 or layer 3 level of protection only, the application layer will be entirely up to the application such as AMHS and SWIM. How IATA is using CRV if so, for the APAC region?

1 Answer:



John Moore Assistant Director, Safety and Flight Operations-ASPAC

International Air Transport Association (IATA) • Submitted on 15 Jun 2021, 12:08

I don't know of any airlines using the CRV yet as SWIM awareness is still evolving slowly for airlines and obviously the COVID interruption meant less priority given to some investments such as SWIM. I expect several of those airlines in ASPAC that are more advanced in their SWIM awareness and planning will be (if not already) involved in tests on things like CRV with ANSPs and MET agencies that are leading the SWIM developments. As far as I know IATA isn't using CRV for any business systems.

1 Comment:

IATA - John Moore • Allowed on 14 Jun 2021, 11:34 • Hidden

I don't know of any airlines using the CRV yet as SWIM awareness is still evolving slowly for airlines and obviously the COVID interruption meant less priority given to some investments such as SWIM. I expect several of those airlines in ASPAC that are more advanced in their SWIM awareness and planning will be (if not already) involved in tests on things like CRV with ANSPs and MET agencies that are leading the SWIM developments. As far as I know IATA isn't using CRV for any business systems.

0 Upvotes | 0 Downvotes

DNS Ecosystem Security

ICAO Asia/Pacific Regional Cybersecurity Webinar

Champika Wijayatunga
Regional Technical Engagement Manager – Asia Pacific

14 June 2021



Agenda

- Overview of the DNS Ecosystem
- DNS Threats and Abuses
- Securing DNS

Overview of the DNS Ecosystem

ASCII Domain Name Labels

www.cafe-123.com



②

Forming ASCII Labels

Use LDH

- Letters [a-z]
- Digits [0-9]
- Hyphen [H]

Label length = 63

①

Forming ASCII Labels

Use only Letters

- Letters [a-z]

Label length = 63

Internationalized Domain Name (IDN) Labels

ตัวอย่าง.ไทย

IDN
second-level
domain

IDN
top-level
domain

Syntax of IDN Labels

Valid U-Label: Unicode code points as constrained by the “LDH” scheme within IDNA 2008

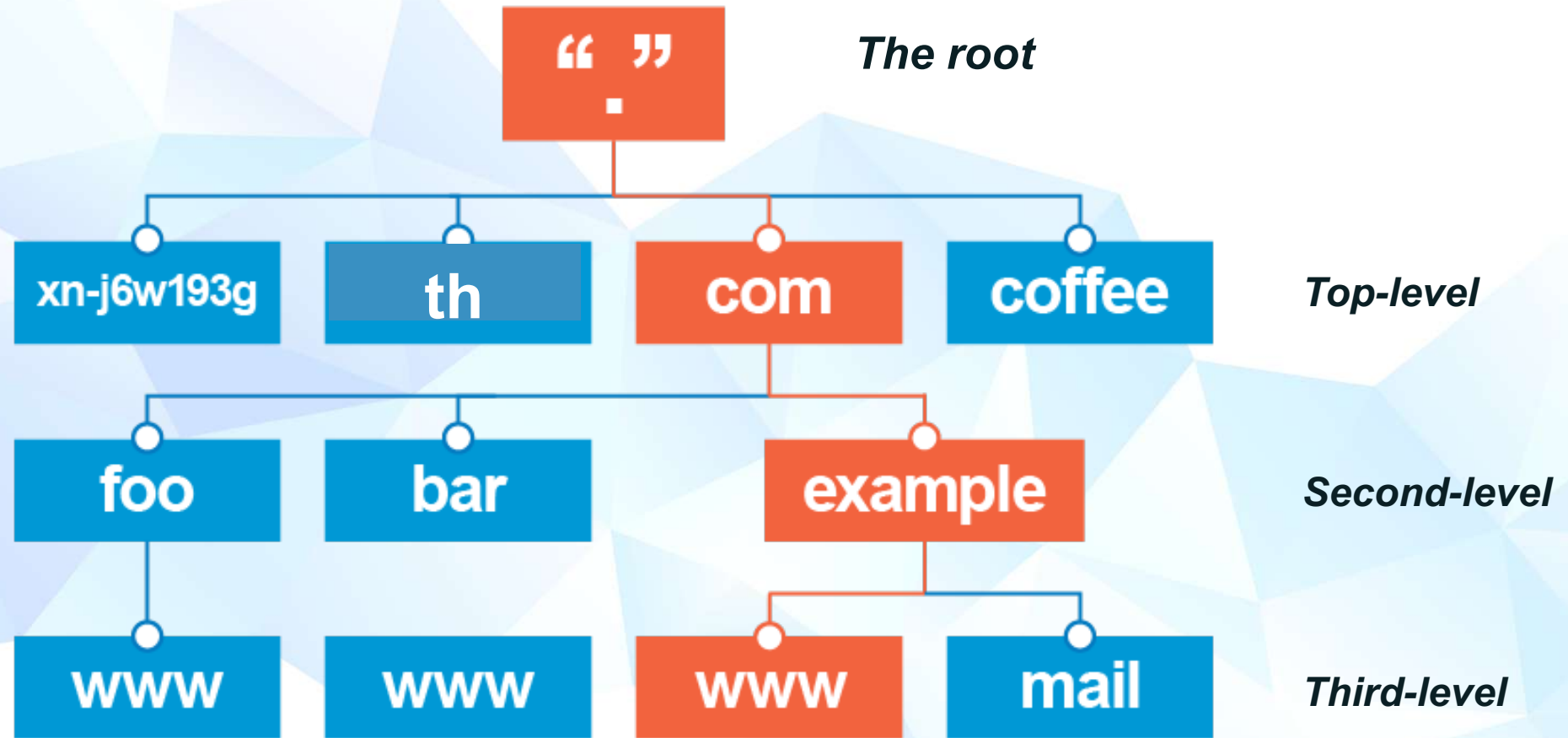
2

Syntax of IDN Labels

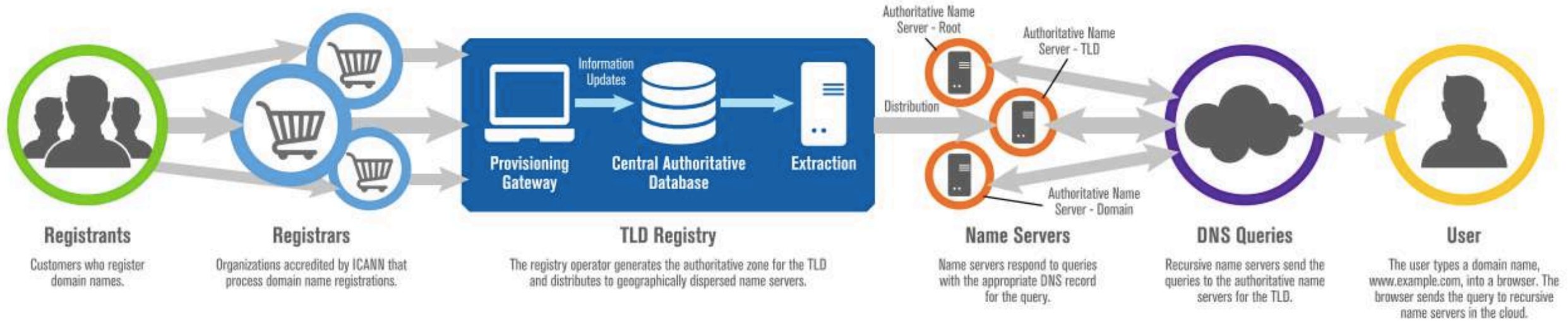
Valid U-label, further constrained by the “letter” principle for TLDs

1

DNS: The Namespace



The DNS Ecosystem



ICANN's Role



Domain Name System

The domain name system provides addressing for the Internet so people can find websites, send email, and other tasks. The ICANN organization also supports the stability of the DNS through its work, and also its contracts and accreditations.



Policy Development

The ICANN organization supports inclusive, open and transparent multi-stakeholder bottom-up consensus based policy development mechanisms.



L-Root

The ICANN organization hosts and supports one of the 13 L-Root infrastructures. At over 160 locations worldwide, L-Root is critical to infrastructure that helps reduce latency and improves performance of the DNS.



Support and Grow the Community

The ICANN organization engages, nurtures and supports interested stakeholders for active and meaningful participation in ICANN. ICANN connects with stakeholders through outreach and engagement, and meeting & event support.



Generic Top-Level Domains

The ICANN organization manages the domain name system's top-level domains. ICANN helps promote competition and choice in the gTLD marketplace.



Country Code Top-Level Domains

The ICANN organization delegates top-level domains identified with a country code. Management is done by national ccTLD operators.



Protocol Parameters

The ICANN organization, in coordination with the Internet Engineering Task Force, manages protocol parameters by maintaining many of the codes and numbers used in Internet protocols.



Internet Protocol Addresses

By serving as the central repository for IP addresses, the ICANN organization helps coordinate how IP addresses are supplied – preventing repetition and conflicts.



Root Zone Management

The ICANN organization helps manage the root zone through the IANA functions, which involves assigning the operators of top-level domains, such as .bank and .com, and maintaining the technical and administrative details.

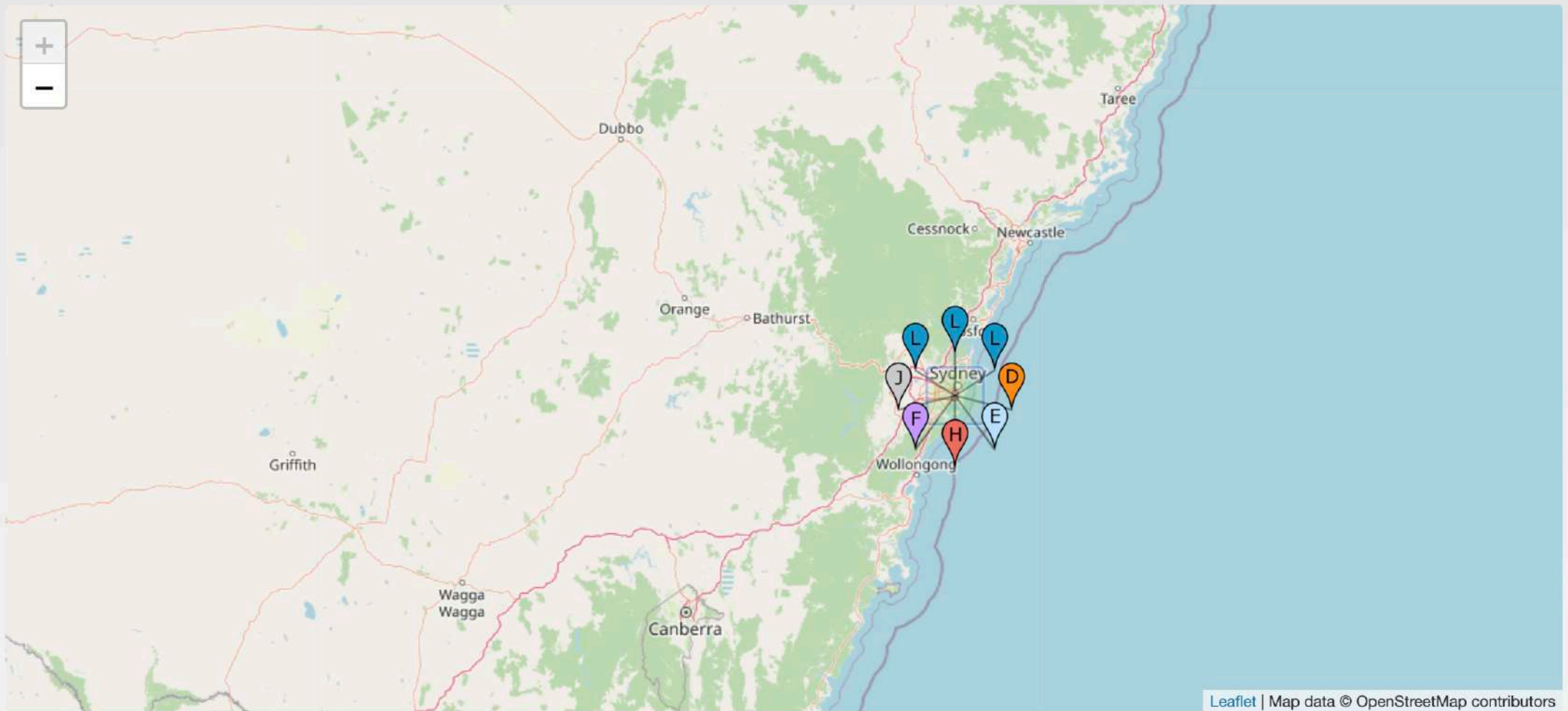
IANA functions

DNS: The Root (Servers)



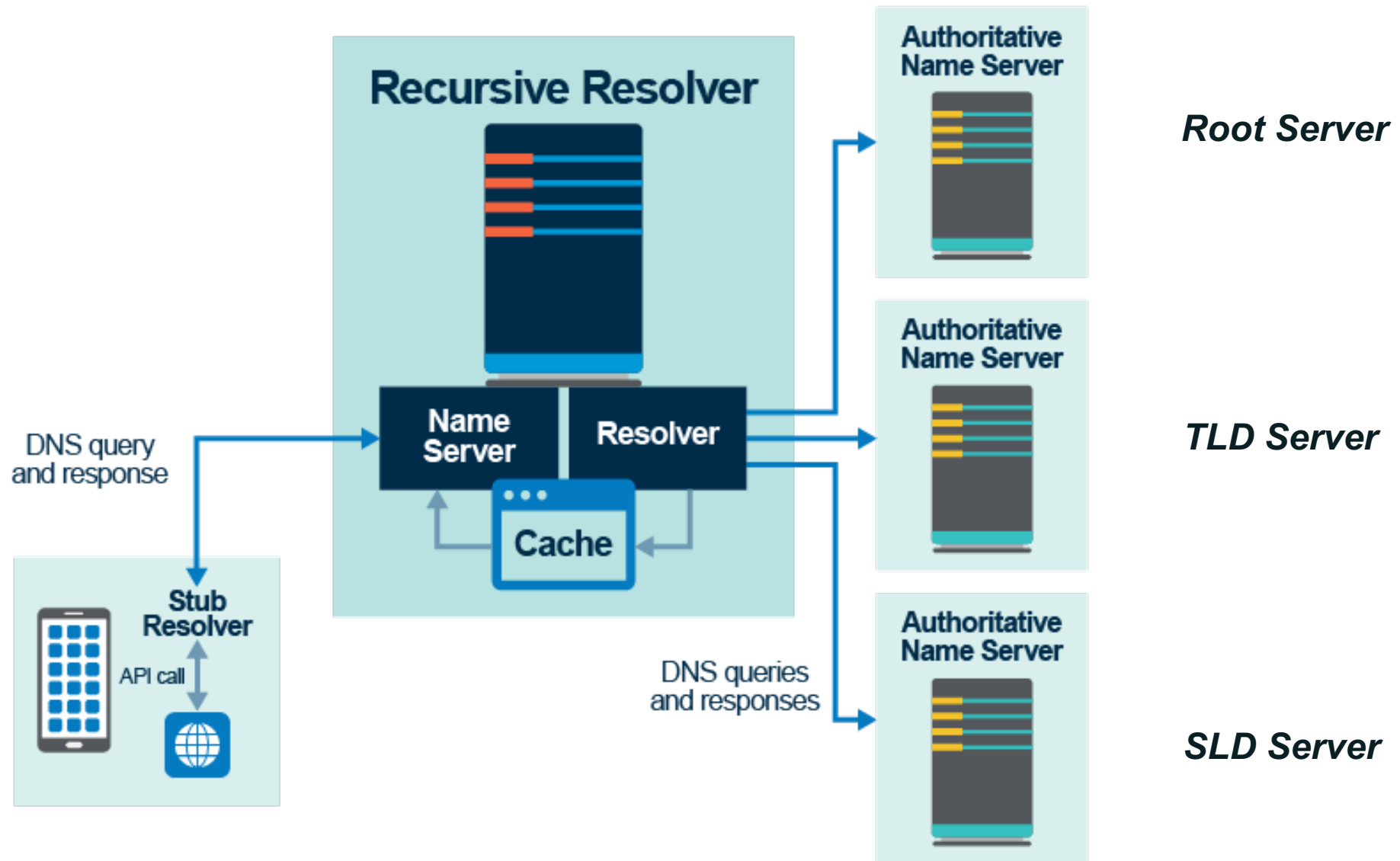
As of 06/08/2021 3:11 a.m., the root server system consists of 1380 instances operated by the 12 independent root server operators.

DNS: The Root (Servers)



As of 06/08/2021 3:11 a.m., the root server system consists of 1380 instances operated by the 12 independent root server operators.

DNS: The Service



DNS Threats and Abuses

DNS contains a wealth of data about your systems

- Your organization's domain names – **example.com**
- Your organization's individual host names –
host.example.com
- IP addresses
- Mail server data (MX records) – **mail.example.com**
- Database locations – **db0.example.com**
- etc

Domain Registrations are Attractive Targets for Attacks

- Automated processes
- Registrar correspondence with registrants largely via emails
- Registrant is responsible for registration data accuracy
- Inexpensive registrations are plentiful
 - Good for consumers but good for attackers too

Namespace Risks

- Homoglyphs
 - **example.com** vs **examp^lé.com** (xn--exempl-gva.com)
 - **aero.com** vs **aero.com** (xn--80agf1b.com)
- Typosquatting
 - **example.com** vs **exmaple.com**

Emojis in Domain Names

Fun, but may be dangerous



https:// 😄 .example

https:// 😁 .example

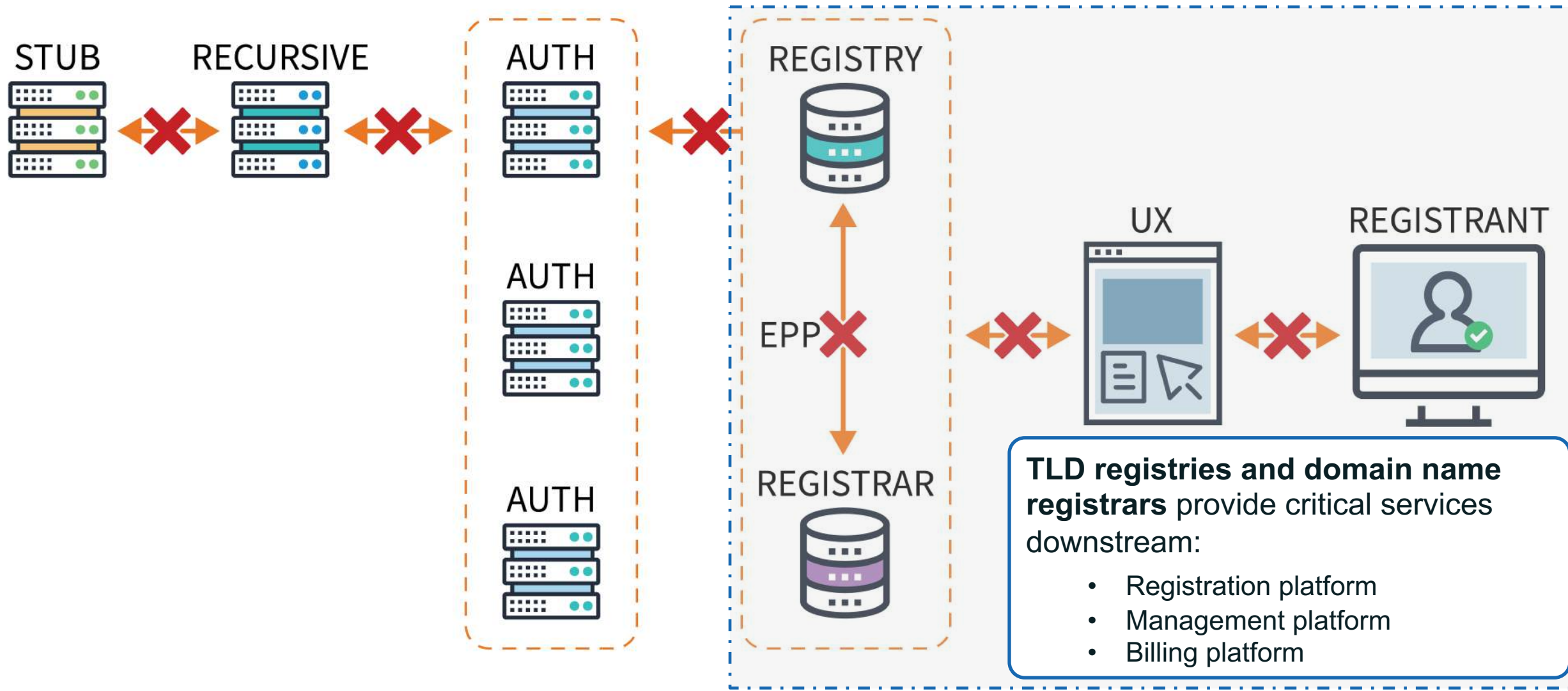
Users could easily confuse the “Grinning face” emoji (left) and “Grinning face with smiling eyes” emoji (right).

⚠️ Emojis can be too visually similar to distinguish especially when displayed in smaller fonts or by different applications ⚠️

Malicious and Misused Domain Registrations

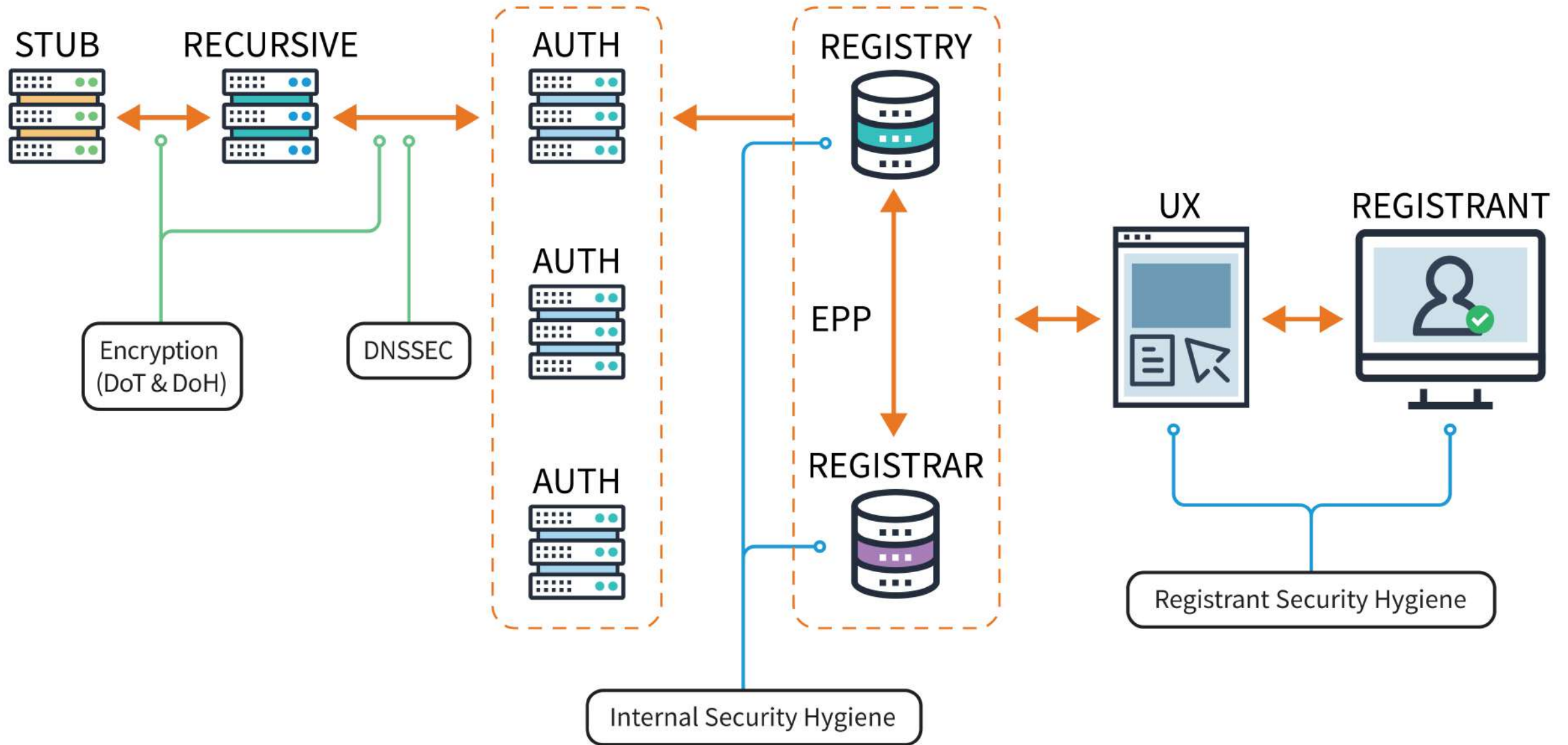
- Phishing
- Business Email Compromises
- Hosting criminal infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism, Exploit attacks
- Malware C&C, Malware distribution
- Cache Poisoning
- Man-in-the-Middle attacks
- etc

Potential Target Points of the DNS Infrastructure/Ecosystem



Securing DNS

A Secure DNS Ecosystem



Best Practices in Securing DNS

- Deployment of DNS Security Extensions (DNSSEC)
- Secure User Interfaces
- Registry/Registrar locks
- Monitoring and diagnostic tools
- Network and Server redundancy
- Secure Zone Transfers (ACLs, TSIG)
- Authoritative Servers must answer authoritatively
- Recursive Servers to provide recursion only to designated clients
- Updated DNS Software
- Support technical standards and compliance
- Know your SLAs
- Have plans in place to deal with attacks and test those regularly
- Good Cyber-hygiene etc.

Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann

Q&A

SP202 – DNS Ecosystem Security

14 Jun 2021, 08:00 - 16:00

by Mr. Champika Wijayatunga Technical Engagement Manager – Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN)

47 Participants 51 Interactions*	36 Total votes 12 Highest vote	7 Questions 7 Allowed 0 Dismissed	7 Questions answered
--	--	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

7 Questions Allowed

12
VOTES

Upal Debnath • 14 Jun 2021 11:14 • ✓ ANSWERED

How DNS eco system may be applied in globalCNS/ATM systems or in SWIM ?

2 Comments:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:43 • Shown

Answered verbally

0 Upvotes | 0 Downvotes

IND_CNS_SATYA • Allowed on 14 Jun 2021, 11:19 • Shown

What is the DNS plan of ICANN to mitigate the cyber threat in Aviation ?

0 Upvotes | 0 Downvotes

8
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 11:09 • ✓ ANSWERED

There were many instances where CDN servers are misconfigured and caused internet outage, how do we prevent such DNS misconfiguration?

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:09 • Shown
Answered

0 Upvotes | 0 Downvotes

6
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 11:17 • ✓ ANSWERED

ICAO intend to use IPv6 for the IATF (Trust Framework), is ICANN already working with ICAO on this?

1 Answer:



Champika Wijayatunga, Technical Engagement Manager

Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN) • Submitted on 15 Jun 2021, 12:09

As ICAO has been receiving IPv4 address space from ARIN you can also request IPv6 from ARIN.

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:09 • Hidden

As ICAO has been receiving IPv4 address space from ARIN you can also request IPv6 from ARIN.

0 Upvotes | 0 Downvotes

4
VOTES

Anonymous • 14 Jun 2021 08:46 • ✓ ANSWERED

You mentioned about some Homoglyphs and Typosquatting, as well as all the phishing practices and compromises. How ICANN protect or action against these malpractices?

1 Answer:



Champika Wijayatunga, Technical Engagement Manager

Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN) • Submitted on 15 Jun 2021, 12:09

DNS Ecosystem is complex and include several stakeholders. Therefore it is important that security best practices should be followed at large rather than a single party. Phishing type of attacks (homoglyphs etc) can be mitigated by deploying DNS Security Extensions (DNSSEC).

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:16 • Hidden

DNS Ecosystem is complex and include several stakeholders. Therefore it is important that security best practices should be followed at large rather than a single party. Phishing type of attacks (homoglyphs etc) can be mitigated by deploying DNS Security Extensions (DNSSEC).

0 Upvotes | 0 Downvotes

3
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 11:12 • ✓ ANSWERED

How do you ensure that DNS queries are not "abused" and carry fileless malware.

1 Answer:



Champika Wijayatunga, Technical Engagement Manager

Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN) • Submitted on 15 Jun 2021, 12:10

Need to deploy DNS firewall type services. (e.g. DNS Response Policy Zones)

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:23 • Hidden

Need to deploy DNS firewall type services. (e.g. DNS Response Policy Zones)

0 Upvotes | 0 Downvotes

2
VOTES

Anonymous • 14 Jun 2021 08:45 • ✓ ANSWERED

If anyone want to learn about DNS/DNS Security in detail what assistance we can get from ICANN?

1 Answer:



Champika Wijayatunga, Technical Engagement Manager

Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN) • Submitted on 15 Jun 2021, 12:11

ICANN provides several capacity building opportunities to the community.

<https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en>Also ICANN has a learning platform called 'ICANN Learn' where you can have access to several training courses. You can create an account at <https://account.icann.org/login> and start accessing ICANN Learn courses.

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:31 • Hidden

ICANN provides several capacity building opportunities to the community.

<https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en>Also ICANN has a learning platform called 'ICANN Learn' where you can have access to several training courses. You can create an account at <https://account.icann.org/login> and start accessing ICANN Learn courses.

0 Upvotes | 0 Downvotes

1
VOTE

Anonymous • 14 Jun 2021 11:13 • ✓ ANSWERED

Is global internet security totally dependent on DNS security? Is the DNS the weakest link on the internet?

1 Answer:



Champika Wijayatunga, Technical Engagement Manager

Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN) • Submitted on 15 Jun 2021, 12:11

Internet Security is much broader. (networks, applications, devices etc.).. DNS a critical part of Internet infrastructure that translates domain or host names to IP addresses, a required process for web navigation, email delivery, and other Internet functions. That is why it is very important to protect your DNS infrastructure to avoid a large attack surface.

1 Comment:

Champika Wijayatunga • Allowed on 14 Jun 2021, 12:42 • Hidden

Internet Security is much broader. (networks, applications, devices etc.).. DNS a critical part of Internet infrastructure that translates domain or host names to IP addresses, a required process for web navigation, email delivery, and other Internet functions. That is why it is very important to protect your DNS infrastructure to avoid a large attack surface.

0 Upvotes | 0 Downvotes

A method of building global mutual trust infrastructure based on Blockchain

Leng Bing

June 2021

Southwest Communications Institute of China

CONTENTS

1. BACKGROUND
2. MUTUAL TRUST ARCHITECTURE
3. ADVANTAGES OF BLOCKCHAIN
4. CAPABILITIES
5. TYPICAL CROSS SECURITY DOMAIN
AUTHENTICATION PROCESS
6. SOFTWARE FUNCTIONAL ARCHITECTURE

Part 1:

BACKGROUND

1. BACKGROUND

- With the evolution of digitalization and the expansion of stakeholders, civil aviation information system is facing more and more **security threats**.
- It is necessary to establish a **global trust cyberspace** of ICAO.
- In this cyberspace, every entity **can be identified** and every behavior **can be expected**.

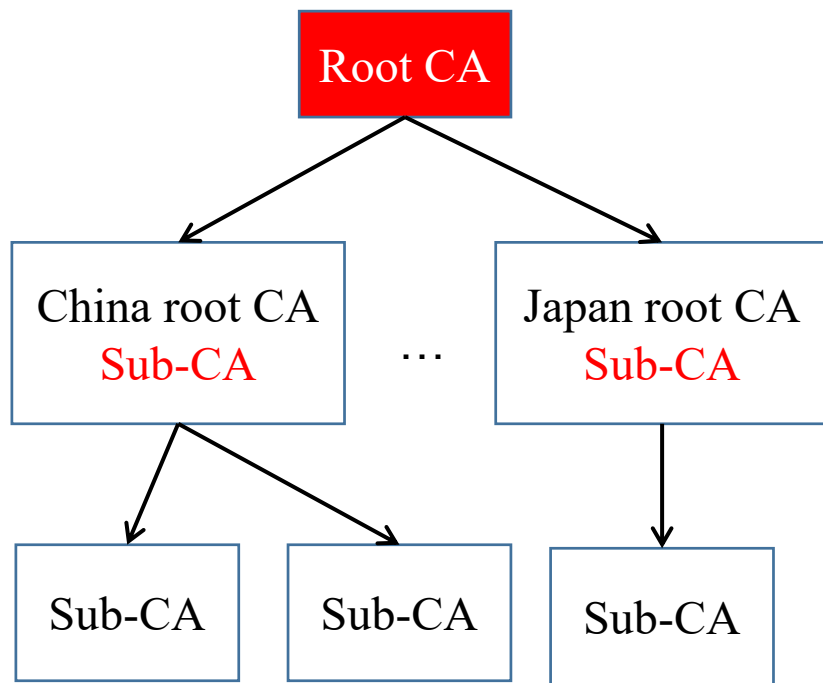
1. BACKGROUND

- The **premise** of CNS (Communications Navigation & Surveillance) is the **identification and mutual trust** between cyberspace entities.
- A Public Key Infrastructure (**PKI**) is a mature and reliable digital identity management system.
- With the help of PKI, **every digital space entity**, *including users, service providers, aircraft, terminals, servers, engines, software, and even data*, **has a unique digital certificate**, just like the **passport** in the physical world.

1. BACKGROUND

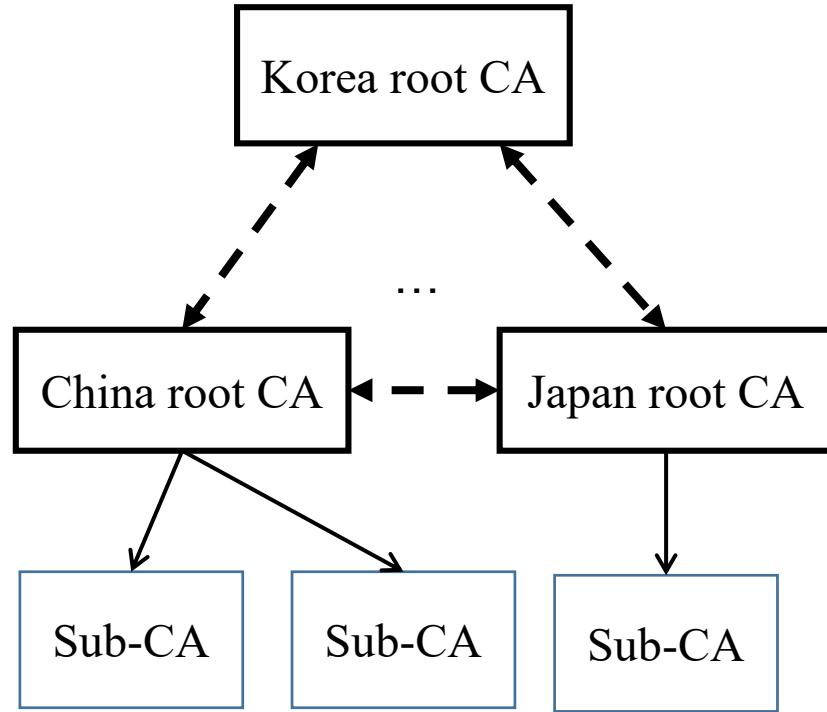
- It is easy to establish a PKI system within a state, the **challenge** is **how to build mutual trust between state PKIs?**
- According to the analysis of the ICAO publication *Global Resilient Aviation Network Concept of Operations*, there are three main architectural approaches to establishing the aviation PKI.

① A single root CA



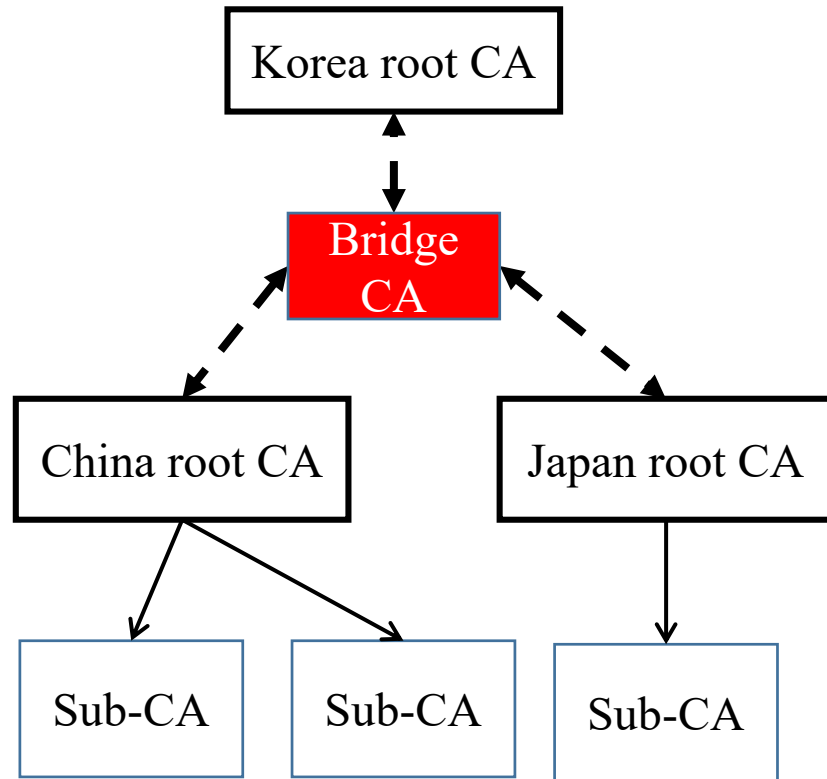
- Add a new root CA (Certificate Authority) beyond the existing root CAs.
- Disadvantage:
 - ① Put the liability of the PKI in the hands of one root CA;
 - ② Every system needs to be modified and reconfigured to adopt the new PKI hierarchy.

② Cross certification between each root CA



- A root CA per state with **individual bi-lateral agreements**.
- **Disadvantage:**
 - ① a root CA per state, region or organization requires the establishment and maintenance of $N * (N-1) / 2$ number of **bi-lateral agreements** between the root CAs.

③ A Bridge CA --Recommended by ICAO publication



- Use a Bridge CA providing bi-directional cross certification **between each root CA and itself**, which can reduce the bi-lateral agreements.
- **Disadvantage:**
 - ① the BCA is **a third party service provider**, the credibility of which determines the reliability of the mutual trust relationship.
 - ② There is **no Trust Third Party** government or organization beyond all member states under current ICAO framework. *—who operate it?*

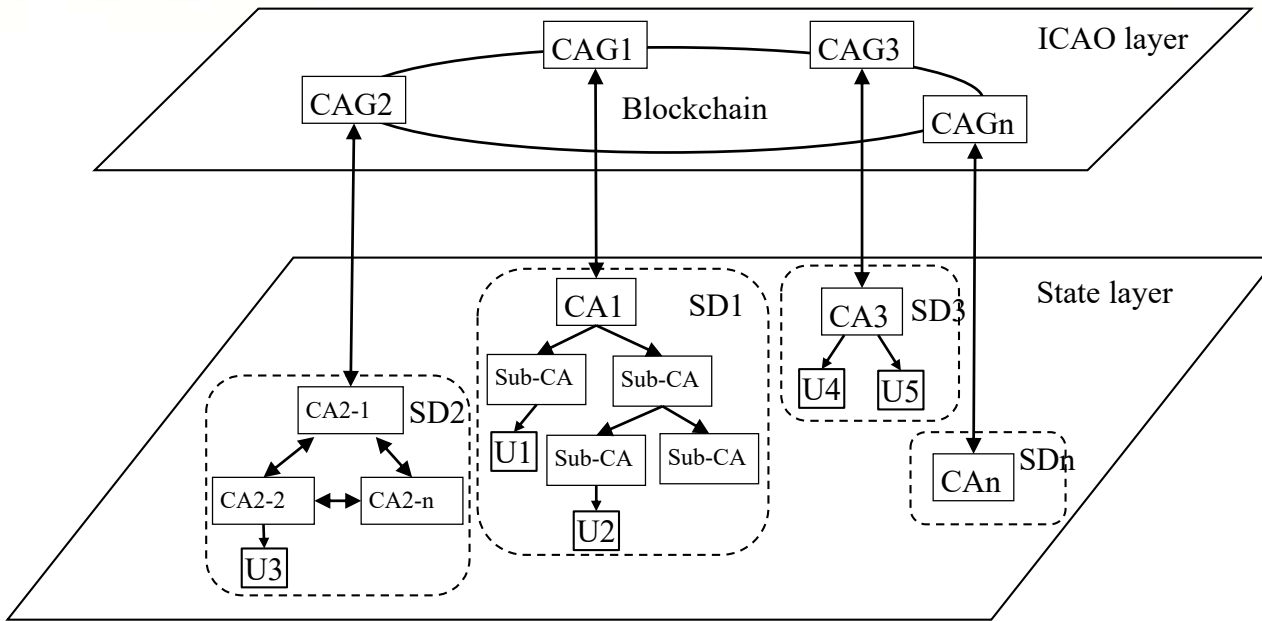
1. BACKGROUND

- Thanks to the latest technology, the **Blockchain** has the characteristics of natural decentralization and can be used for the construction of Mutual Trust Infrastructure among global states.
- At ICAO-UAE blockchain Summit and Exhibition, held on 3-4 April 2019 in Dubai, **ICAO Council President Dr. Aliu** underscores that:
 - Blockchain has the potential to enhancing both safety and security.
 - I am looking forward to some provocative ideas and insights from our key presenters.

Part 2:

MUTUAL TRUST ARCHITECTURE

Mutual trust architecture



- ICAO layer consists of CA Gateway(CAG) of each member state, which is a distributed and decentralized alliance blockchain. --*Simple deployment*
- Each state is an independent Security Domain and can adopt different PKI architectures. The existing PKI infrastructure does NOT need to be modified or reconfigured. --*Good compatibility*
- Each CAG node is managed by its own state, and a CAG provides bi-directional cross certification between a root CA and itself. --*Clear management*
- The digital certificates of all level CAs of each state and the Certificate Revocation List(CRL) should be stored in the blockchain. --*Clear function*

Part 3:

ADVANTAGES OF BLOCKCHAIN

3 ADVANTAGES OF BLOCKCHAIN

3.1 Transparent and trustworthy

- In the blockchain system, all nodes are peer-to-peer nodes. Everyone sends and receives messages equally in the network, so each node can observe all the behaviors of nodes in the system completely, and the whole system is transparent to each node.
- The final result is obtained by all nodes using a consensus algorithm.

3 ADVANTAGES OF BLOCKCHAIN

3.2 Tamper proof and traceable

- In the blockchain, once the operation is written, it cannot be tampered.
- Any operation on the blockchain has a complete record and can be traced.

3 ADVANTAGES OF BLOCKCHAIN

3.3 High reliability

- Firstly, each node maintains an account book equally and participates in the consensus of the whole system. The failure or offline of one node will not affect the normal operation of the whole system.
- Secondly, the blockchain system supports Byzantine Fault Tolerance. Even if there are a certain number of malicious attack nodes in the system, the system can operate normally.

Part 4:

CAPABILITIES

4. CAPABILITIES

The system should:

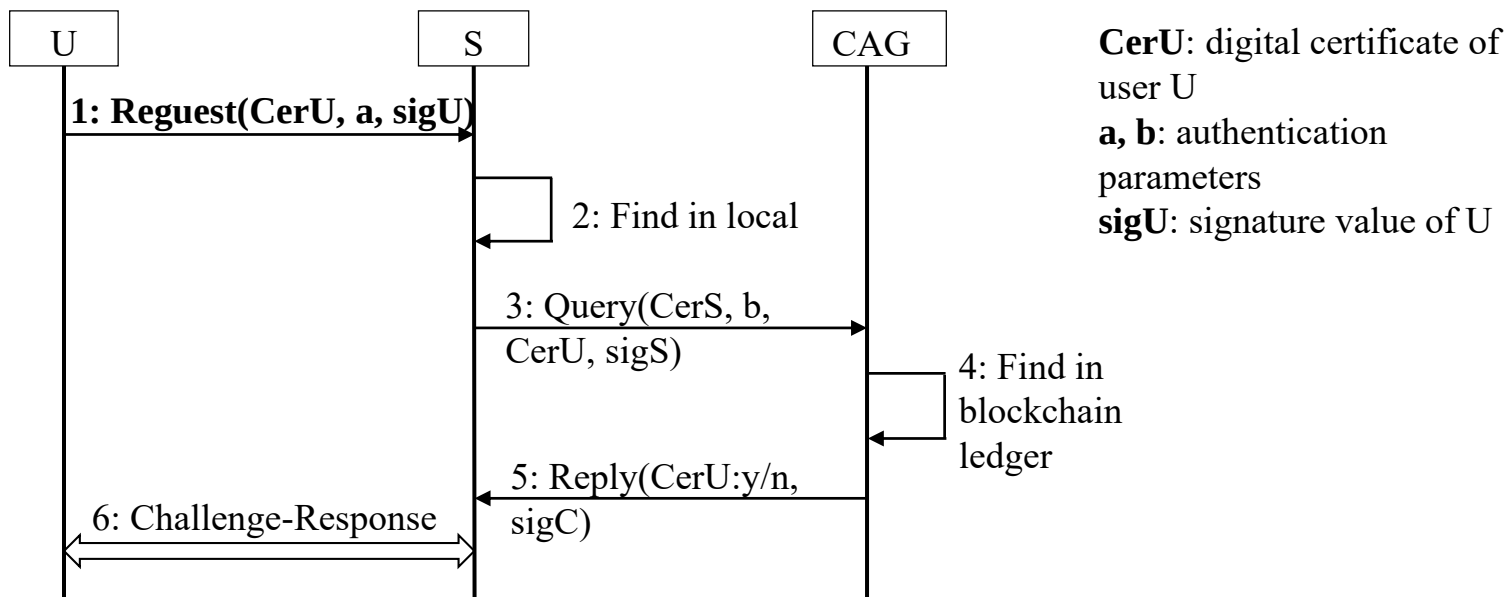
- (1) Support digital certificate storage, retrieval, verification, update, revocation and other operations.
- (2) Provide web service interface;
- (3) Blockchain building capacity of no less than 500 CAG nodes.
- (4) The certificate query time on the Blockchain is less than 5 seconds.
- (5) The certificate verification time is less than 1 second.
- (6) The query time of certificate revocation list on the blockchain is less than 5 seconds.

Part 5:

**TYPICAL CROSS SECURITY DOMAIN
AUTHENTICATION PROCESS**

Typical cross Security Domain authentication process

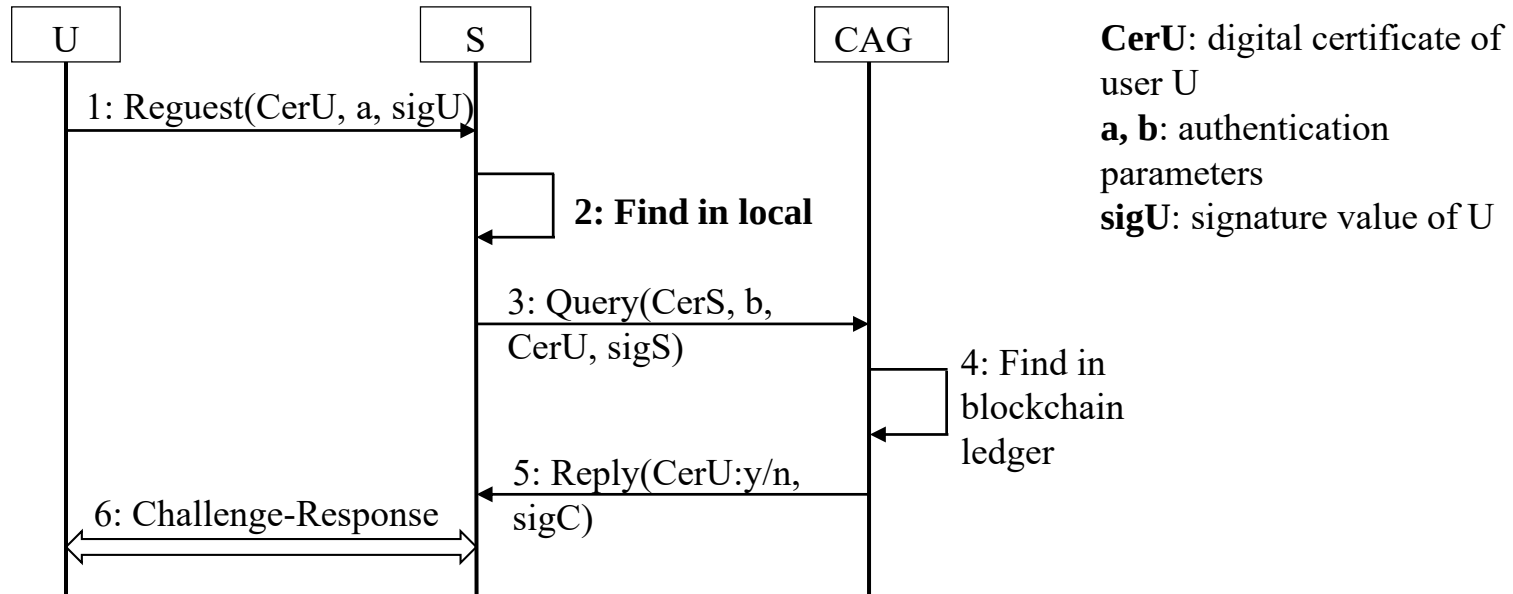
Use Case: a user U in Korea wants to access a server S in China.



Step1: User U send access request to Server S. The digital certificate of U is contained in the request package.

Typical cross Security Domain authentication process

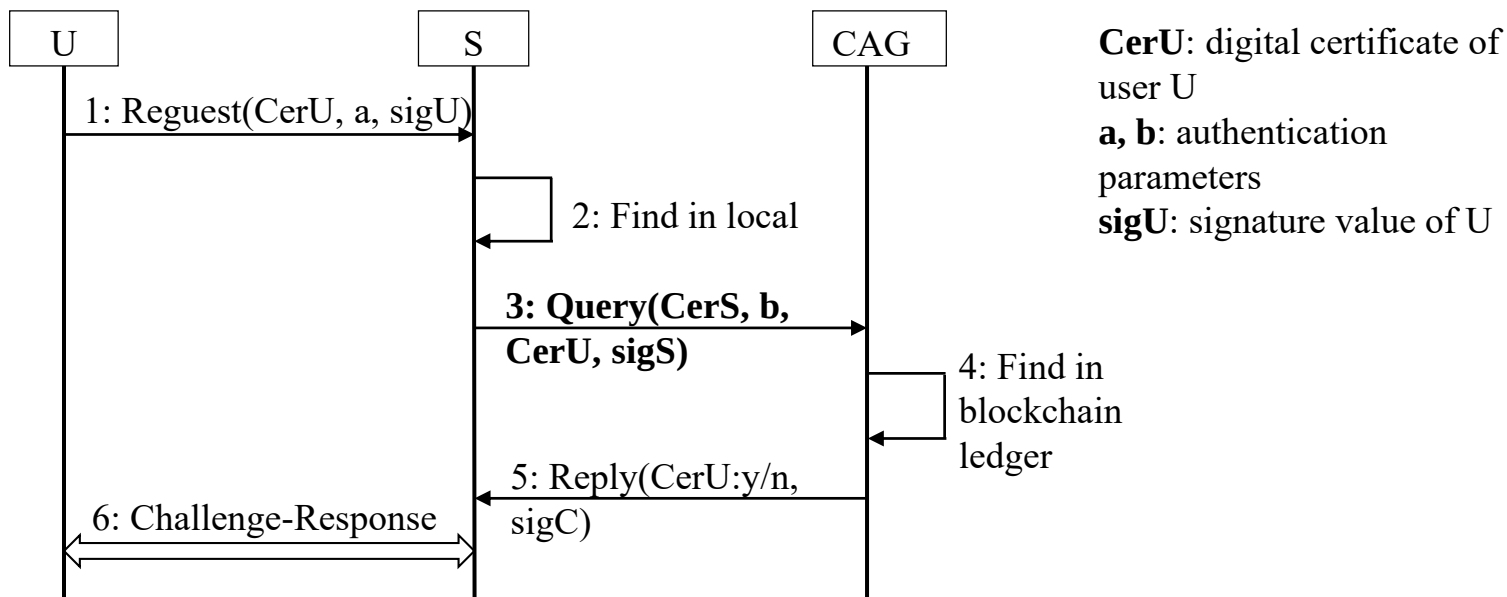
Use Case: a user U in Korea wants to access a server S in China.



Step2: Server S tries to find the public key of the CA who issued the digital certificate of U in its local cache.

Typical cross Security Domain authentication process

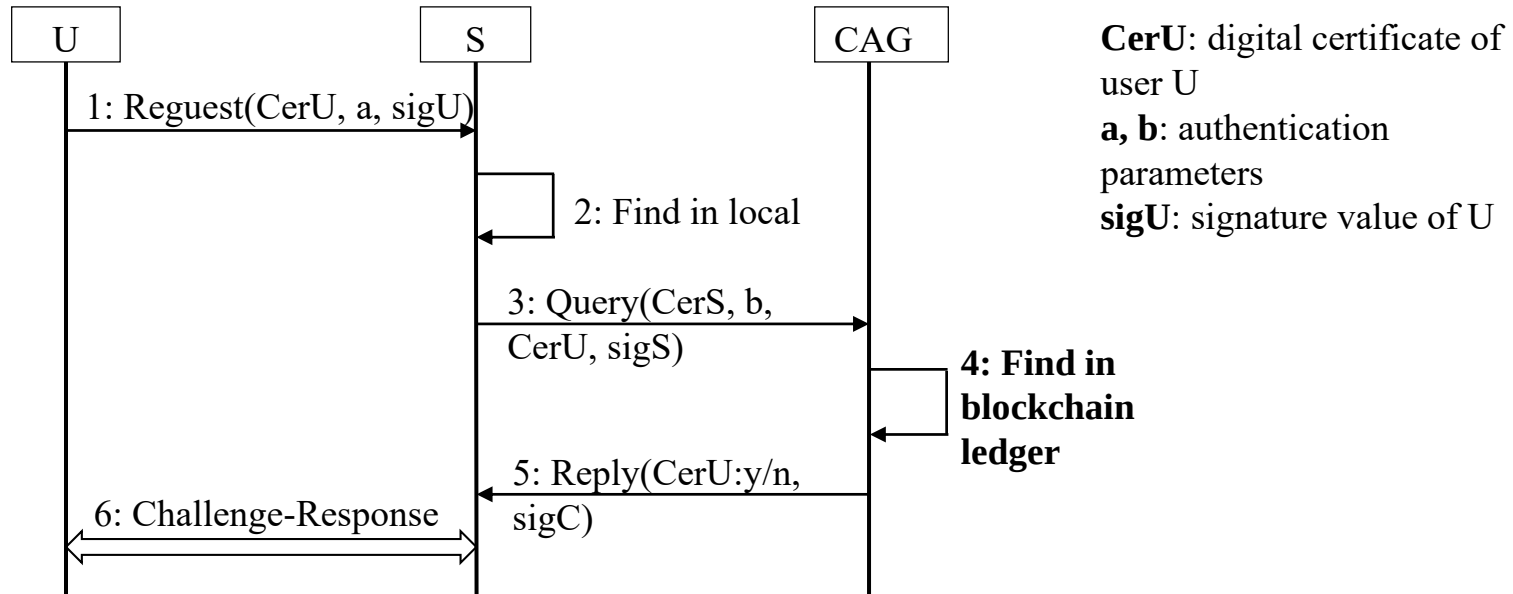
Use Case: a user U in Korea wants to access a server S in China.



Step3: If S has not found the right public key, it can not validate the truth of digital certificate U, so S refers to CAG of China for help.

Typical cross Security Domain authentication process

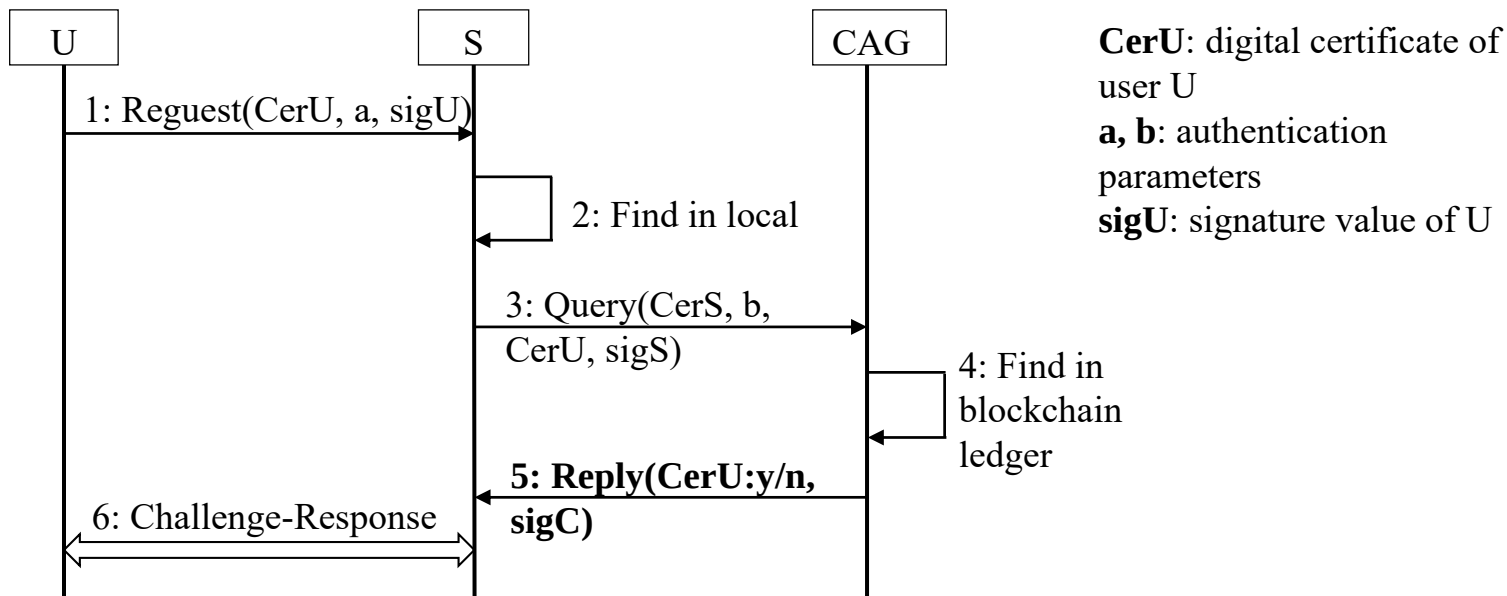
Use Case: a user U in Korea wants to access a server S in China.



Step 4: When receiving the query from S, the CAG of China will search for the public key of the CA who issued the digital certificate of U in the blockchain ledger according to the IssuerUniqueID. With the help of the public key of CA, CAG can validate the truth of digital certificate U. At the same time the certificate revocation list is queried to ensure that digital certificate U has not been revoked.

Typical cross Security Domain authentication process

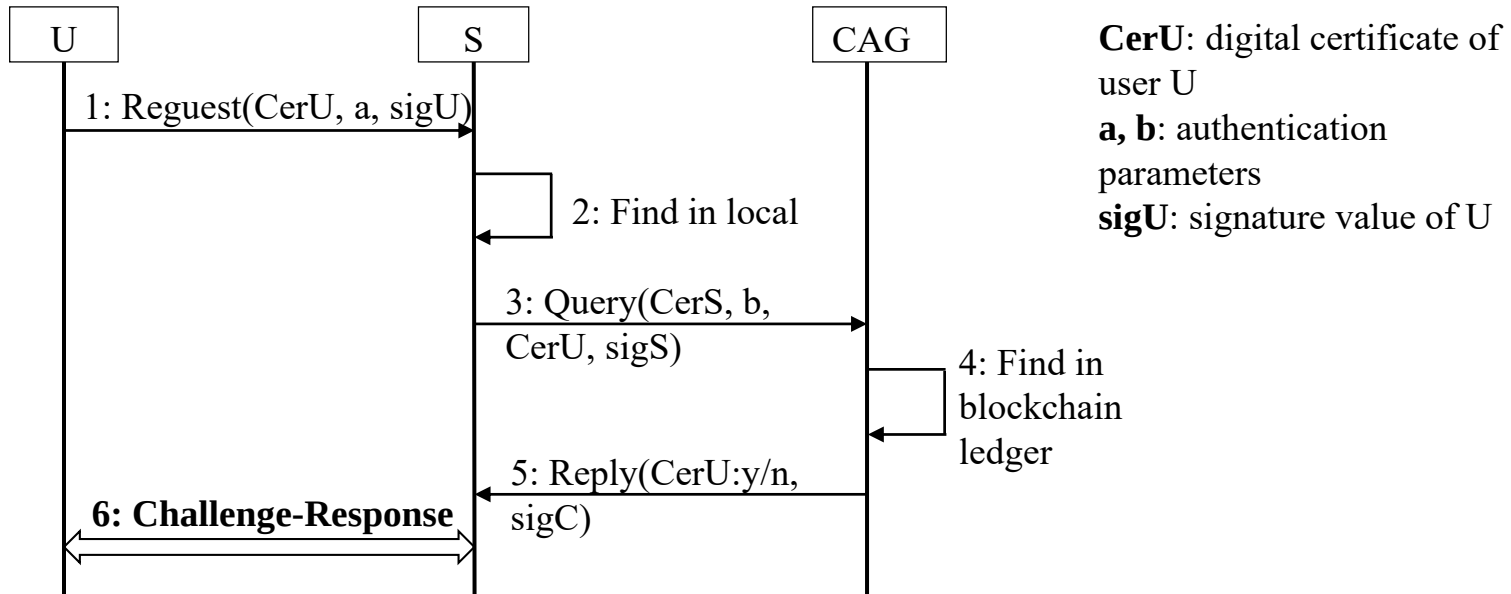
Use Case: a user U in Korea wants to access a server S in China.



Step5: The CAG reply S the validity of the digital certificate U.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.



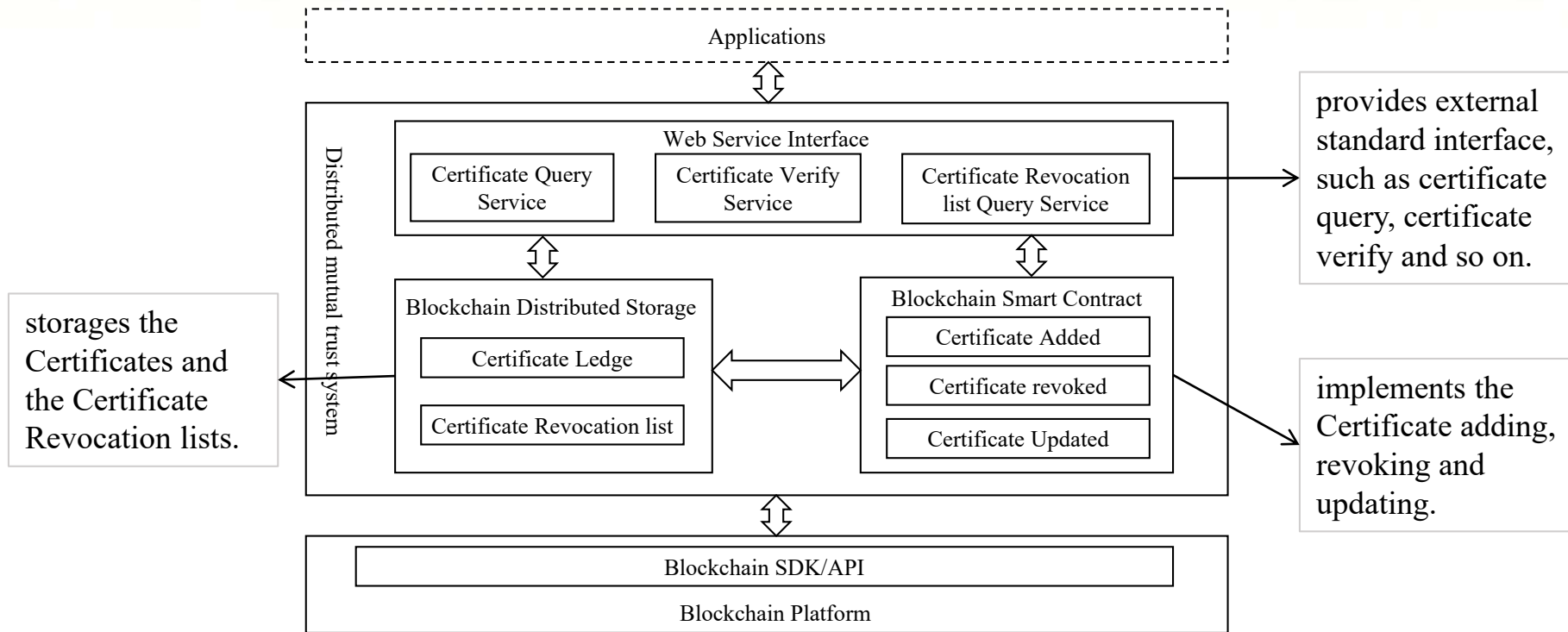
Step6: After S knows the digital certificate U is valid, it can initiate the subsequent challenge-response authentication process.

Part 6:

SOFTWARE FUNCTIONAL

ARCHITECTURE

Software Functional Architecture



- The bottom layer provides basic functions of blockchain, which exposes the blockchain APIs.
- The middle layer is a distributed mutual trust system, which is composed of three parts.
- The upper layer uses the distributed mutual trust system for security protection, such as Flight Plan Filling.

THANK YOU

Contact information:

Leng Bing,
Southwest Communications Institute of China
Address: Chengdu, Sichuan, China
Tel: +86-13980086683
Email: lengbing@tom.com

 Q&A

SP203 – Building Mutual Trust Infrastructure Based on Block Chain

14 Jun 2021, 08:00 - 16:00

by Mr. Leng Bing Principal Researcher, Southwest Communications Institute of China

40 Participants 19 Interactions*	14 Total votes 6 Highest vote	5 Questions 5 Allowed 0 Dismissed	5 Questions answered
--	---	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

5 Questions Allowed

6
VOTES

Anonymous • 14 Jun 2021 09:53 • ✓ ANSWERED

The presentation is technical and concise. How would you suggest to incorporate such blockchain based framework to existing infrastructure like CRV and SWIM?

1 Answer:



Leng Bing, Principal Researcher

Southwest Communications Institute of China • Submitted on 14 Jun 2021, 12:49

Trust infrastructure is the underlying system of all application systems, including CRV and SWIM. You can integrate this trust infrastructure into the bottom layers of CRV and SWIM. When CRV and SWIM need transnational authentications, they can call the trust infrastructure service. Of course, because each state is an independent security domain and different PKI systems may be deployed. So the authentication between users and services within a state does not need to call the trust infrastructure services between states.

5
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 11:54 • ✓ ANSWERED

Blockchain is still new and adoption is basically on crypto currency, but will ICAO consider this over PKI?

1 Answer:



Leng Bing, Principal Researcher

Southwest Communications Institute of China • Submitted on 14 Jun 2021, 13:04

Blockchain comes from bitcoin in 2009. When it was born, its built-in script system was specially designed for encrypted digital currency. In order to support the application of non encrypted digital currency, smart contract is introduced in blockchain 2.0 to support user-defined business logic. So, the application of blockchain has expanded from the initial encrypted digital currency to cross-border clearing, supply chain, government affairs, digital rights and other fields. Blockchain has many successful practices. The problem of transnational trust building is the lack of a trusted third party. Blockchain technology is not used to replace PKI in ICAO. On the contrary, blockchain technology can be used to supplement PKI system in this aspect. They can work together. Blockchain works in ICAO layer and PKI works in state layer.

2
VOTES

Anonymous • 14 Jun 2021 12:01 • ✓ ANSWERED

One of the problem with PKI is outdated CRL or OSCP latency in querying revoked certificate. Does blockchain help improve the situations

1 Answer:



Leng Bing, Principal Researcher

Southwest Communications Institute of China • Submitted on 14 Jun 2021, 13:14

No, blockchain can't solve this problem. Blockchain technology can be used to link the trust of root CA and extend the ability of PKI. The latency problem of CRL and OSCP needs to be solved by PKI itself.

1
VOTE

Anonymous • 14 Jun 2021 09:49 • ✓ ANSWERED

With recent craze of Bitcoin, crypto topics seems a hit. What is the relationship between a virtual digital cryptocurrency technology and establishment of mutual trust infrastructure among APAC states

1 Answer:



Leng Bing, Principal Researcher

Southwest Communications Institute of China • Submitted on 14 Jun 2021, 13:06

Yes, blockchain comes from bitcoin, but bitcoin is only one of its applications. The development of blockchain includes three stages. They are encrypted digital currency, enterprise application and value Internet. The similarity between bitcoin and trust infrastructure lies in that they both need to establish a trust relationship between cyberspace entities without a trusted third party. This is exactly what blockchain technology is good at.

0
VOTES

Anonymous • 14 Jun 2021 09:58 • ✓ ANSWERED

Is there any trial projects already implemented and what are the challenges?

1 Answer:



Leng Bing, Principal Researcher

Southwest Communications Institute of China • Submitted on 14 Jun 2021, 13:18

As far as I know, there is no relevant project in the field of civil aviation. However, there are many mature applications in other fields, such as supply chain, government affairs, digital rights, certificate keeping, etc. The challenge is to understand the business application itself. You should find out the combination of the advantages of blockchain and business logic. For example, someone directly uses blockchain in real-time authentication system, and it turns out that blockchain is not fast enough. Therefore, in my proposed trust infrastructure, blockchain is mainly used to store digital certificates, not directly participate in every real-time authentication.



ICAO Asia/Pacific Regional Cybersecurity Webinar
“Management Framework for CNS/ATM Systems”
14 June 2021

**A Proactive and Systematic Approach in Protecting Digitized
Air Traffic Services against Cyber Threats
in Hong Kong from ANSP and Regulatory Perspective**

Presented by Hong Kong, China

Regulatory Perspective

Regulatory Perspectives

- Aviation Cybersecurity under Regulatory Regime in Hong Kong
 - HKASP Section 6.10 – Measures relating to Cyber Threats (Reference Annex 17 SARPs 4.9.1, 4.9.2)
 - Submission of Cybersecurity Programme by Air traffic control service provider.

Security Plan for Air Traffic Services

- Uphold a common baseline to work towards Cybersecurity Standards and Recommended Practices

(Reference: Chapter 18 , Doc 8973)

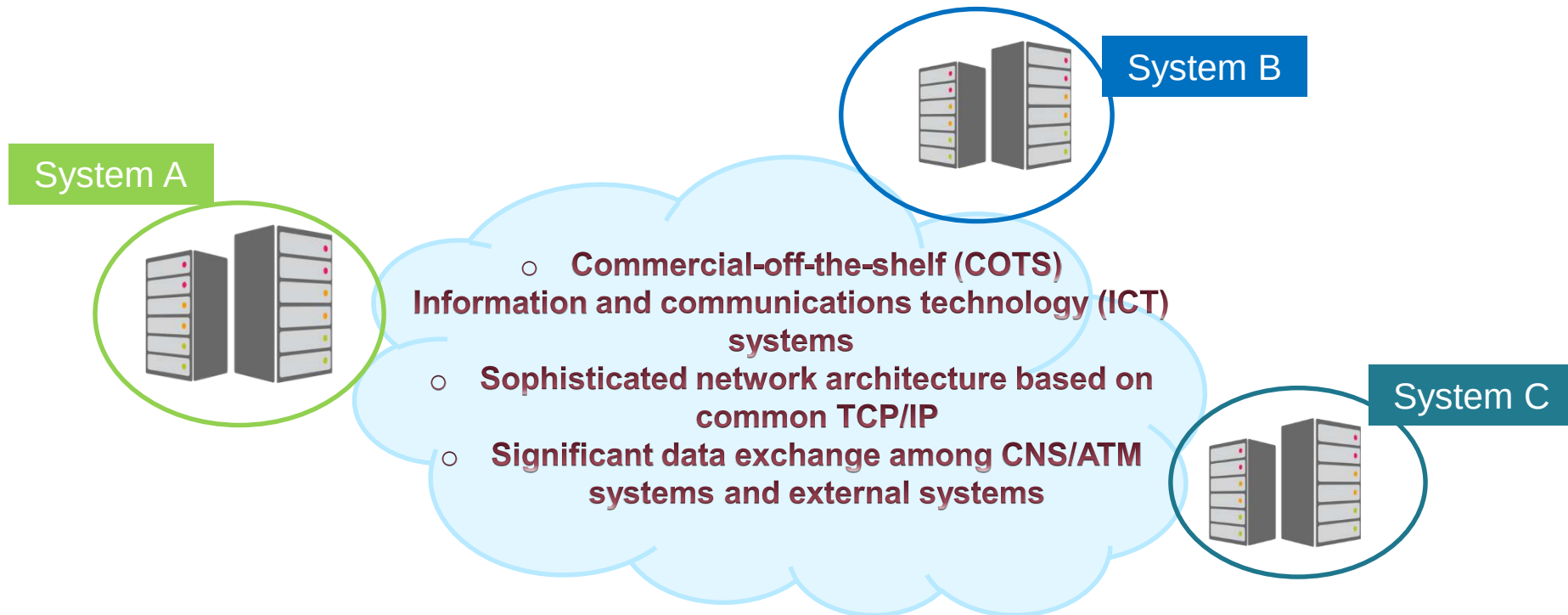


Service Provider Perspective

Introduction

■ New Generation of Air Traffic Services (ATS)

- High level of digitization
- Increasing interconnectivity



Introduction

■ The Challenge for ANSPs:

- Cyber threats might impact the safety and security of Air Traffic Services.

■ Objectives

- Protecting information data and physical assets against cyber threats
- A proactive and systematic approach in implementation of cyber security measures to protect ATS from cyber threats.

Cyber Security Management in HKCAD

- HKCAD achieving the objectives by:
 - Setting up a cyber security management;
 - Managing cyber security processes in a proactive and systematic manner; and
 - Ensuring that all significant cyber threats risks to ATS are adequately addressed and mitigated.

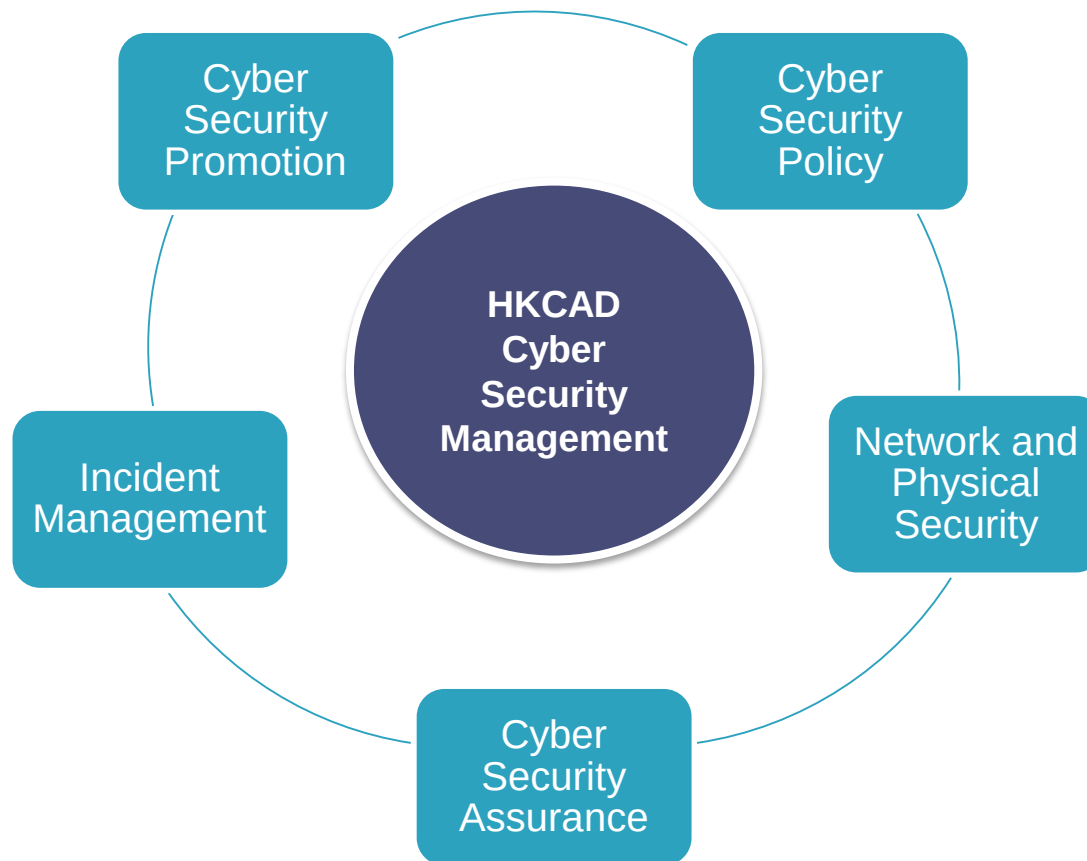
Cyber Security Management in HKCAD

Establishment of CAD ANS Cyber Security Committee (CACSC)

- Regular meetings to set out policies and steer the implementation of cyber security control measures throughout the whole life cycle of the ATS systems.
- Committee members are from various perspectives (regulatory, operational and technical staff)

Cyber Security Management in HKCAD

- The key cyber security processes under HKCAD cyber security management are as follows:



Cyber Security Policy

■ Documented Policy and Procedure

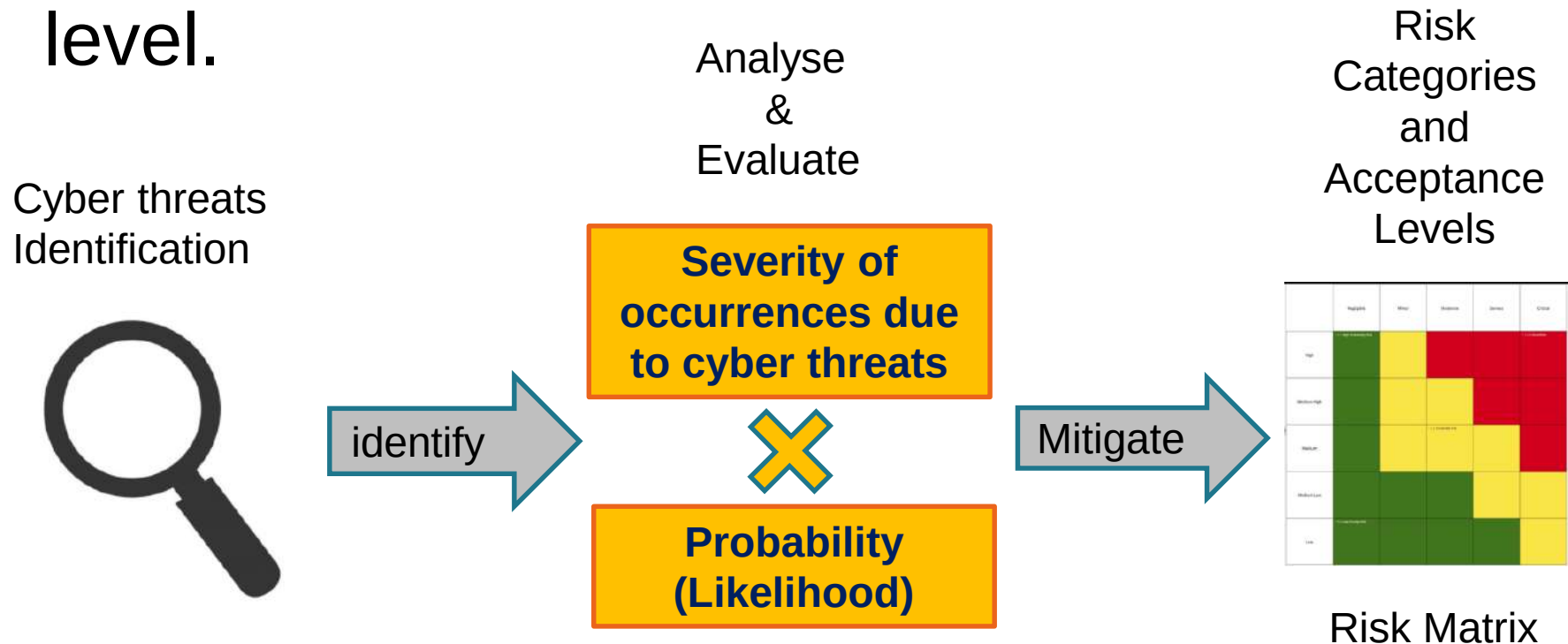
- Developed documentation in accordance with ICAO Annex 17, Doc 9985 and Doc 8973
- Provide protection of safety-critical ATS systems against cyber threats
 1. Cyber Security Manual
 2. Cyber Security Handbook
 3. User Account Management Policy for ATS
 4. Security Plan

Cyber Security Policy

- The “**Identify**” element of the framework is included in defining the security policy.
- A list of core ATS systems was identified with reference to risk management assessment process and business need, then documented the applicable scope in the policy.
- Based on the cyber threat risk management, business needs to prioritize the organisational efforts to implement physical and cyber security measures.

Risk Management

- Established cyber security assessment processes to identify hazards, and analyse, evaluate and mitigate risk to an acceptable level.



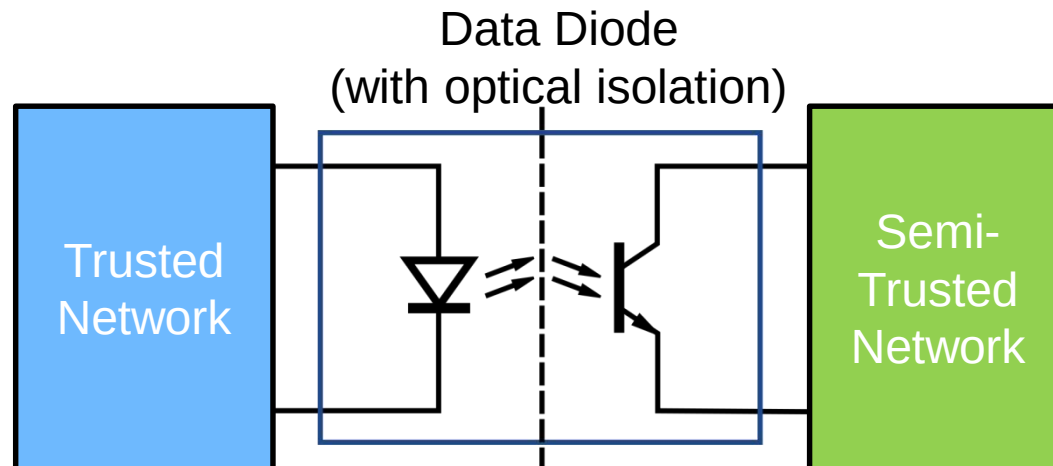
Network Security

- The “**Protect**” element of the framework is included in this process.
- ATS Systems interconnected for information exchange.
- Connection via a common Internet Protocol (IP) data network, Air Traffic Control Data Network (ATCDN)
 - Multi-tier defence-in-depth scheme
 - Network equipment with firewalls, Network Intrusion Detection System (NIDS) or Network Intrusion Prevention System (NIPS) to guard against external connections
 - Data Diode to allow uni-directional communication

Network Security

■ Data Diode Network

- Restrict uni-directional communication from trusted zone to semi-trusted zone
- Optical isolation at transmitting and receiving ends
- Uses for dissemination of surveillance multicast data



Network Security

■ Removable Media Control

- Common route for importing malicious content to information system.
- Restrict the use of removable media
- Media are scanned for malicious content by the machine prior to uploading data to ATS systems.

Physical Security

■ Physical Security Measures

- Multi-layer approach
- From perimeter security down to console/rack level
- Control measures include:
 - Facility management
 - Security guards
 - CCTV surveillance
 - Room access control
 - Physical lock, etc.

Cyber Security Assurance

- The “**Detect**” element of the framework is included in this process.
- Performance Monitoring and Measurement
 - External and Internal Audit
- Continuous Improvement
 - Software Security Patch Management
 - Assess the requirements of security vs system performance.
 - Work closely with system manufacturers to evaluate system patch when considered appropriate.

Incident Management

- The “**Response**” & “**Recover**” element of the framework are included in this process.
- Established the escalation procedure of cyber security incidents
 - Work closely with Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF).
 - Direct reporting mechanism has established for HKCAD to seek swift assistance from CSTCB.
 - CSTCB provides advice and independent assessment on cyber security measures implemented.
 - Conduct drill exercises to keep up staff awareness and ensure the robustness of the response planning and recovery planning.

Incident Management

- The Joint Cyber and Physical Security Drill with HKPF was conducted at CAD Headquarters in April 2021 to enhance our response capability.
 - A storyline included both cyber and physical security incident to practice an all-rounded response.
 - Discovery, incident response and investigation activities were drilled to strengthen our readiness.



Cyber Security Promotion

- Staff awareness is essential to implement cyber security.
 - HKCAD provides cyber security training to our staff regularly to strengthen their awareness of cyber security.
 - HKCAD staff also raise their security awareness by participating in security drills, conference and seminars.



Thank you

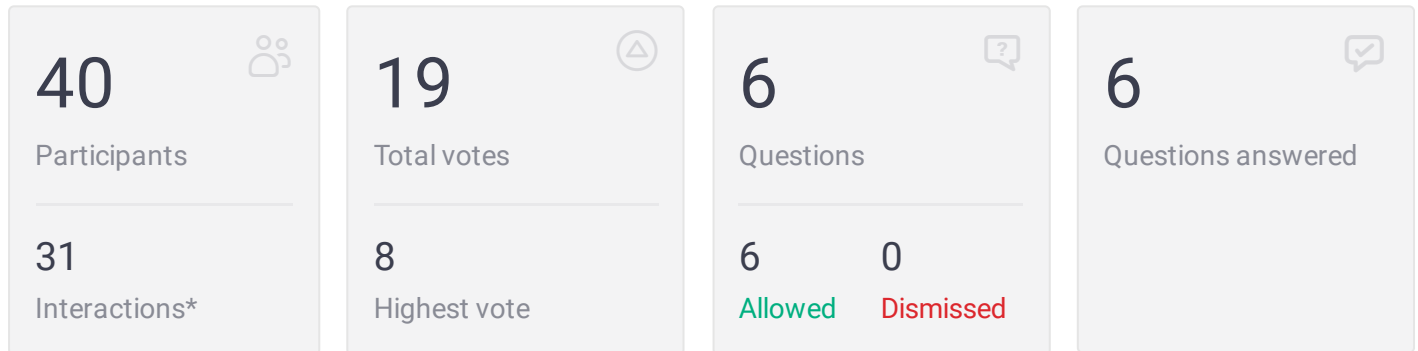


 Q&A

SP301 – A proactive and systematic approach in protecting digitized air traffic services against cyber threats in Hong Kong from ANSP and regulator

14 Jun 2021, 08:00 - 16:00

by Mr. Raymond Chan Senior Electronics Engineer, Civil Aviation Department (CAD), Hong Kong, China



* Interactions include the total number of questions, votes, comments and answer ratings

6 Questions Allowed

8
VOTES

Anonymous • 14 Jun 2021 08:35 • ✓ ANSWERED

What is the benefit of using data diode? What is the difference between the use of a traditional firewall and data diode?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:13

The optical data diode is a hardware-based secure device that allows data to travel in only one direction. The optical data diode is comprised of a laser diode as a data transmitter (upstream), and the laser is directed to the receiving end (downstream). There is no way to allow reverse data traffic in a data diode. A firewall could allow two-way data flow. Iso, it depends on the data flow and data type. Not all data interfaces can use a data diode to isolate the traffic. Multicast traffic without return traffic data flow is an example of using a data diode.

1 Comment:

Raymond Chan • Allowed on 14 Jun 2021, 15:05 • Hidden

The optical data diode is a hardware-based secure device that allows data to travel in only one direction. The optical data diode is comprised of a laser diode as a data transmitter (upstream), and the laser is directed to the receiving end (downstream). There is no way to allow reverse data traffic in a data diode. A firewall could allow two-way data flow. Iso, it depends on the data flow and data type. Not all data interfaces can use a data diode to isolate the traffic. Multicast traffic without return traffic data flow is an example of using a data diode.

0 Upvotes | 0 Downvotes

4
VOTES

Anonymous • 14 Jun 2021 10:19 • ✓ ANSWERED

The model in Hong Kong shows a full implementation of Lead-Identify-Protect-Detect-Respond-Recover. Were there any actual threats monitored/discovered and how your org dealt with it?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:13

From monitored and discover, HKCAD has 7x24 round-the-clock network operation centres to monitor the network status. The centres are manned and the staff make use of network monitoring tools, such as SIEM, to check for a cyber incident. Luckily, we do not have actual threats faced so far. Our incident response procedures are performed in drill exercises, and our staff are vigilant in detecting cyber security incidents.

1 Comment:

Raymond Chan • Allowed on 14 Jun 2021, 15:04 • Hidden

From monitored and discover, HKCAD has 7x24 round-the-clock network operation centres to monitor the network status. The centres are manned and the staff make use of network monitoring tools, such as SIEM, to check for a cyber incident. Luckily, we do not have actual threats faced so far. Our incident response procedures are performed in drill exercises, and our staff are vigilant in detecting cyber security incidents.

0 Upvotes | 0 Downvotes

3
VOTES

Anonymous • 14 Jun 2021 12:58 • ✓ ANSWERED

Does the Cyber Security Policy refer to ISO 270xx series and NIST?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:13

CAD fully supports ICAO cyber security initiatives and documentations. Some common security frameworks such as ISO 27000 and NIST are good practice for reference.

1 Comment:

Raymond Chan • Allowed on 14 Jun 2021, 15:05 • Hidden

CAD fully supports ICAO cyber security initiatives and documentations. Some common security frameworks such as ISO 27000 and NIST are good practice for reference.

0 Upvotes | 0 Downvotes

2
VOTES

Anonymous • 14 Jun 2021 13:10 • ✓ ANSWERED

How is the key difference between Network Security and Cyber Security?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:12

Cyber Security is considered the security threat is focusing more on internet-connected systems. Network security is considered the protection of assets and data from the network in general.

1 Comment:

Anonymous • Allowed on 14 Jun 2021, 15:06 • Hidden

Cyber Security is considered the security threat is focusing more on internet-connected systems. Network security is considered the protection of assets and data from the network in general.

0 Upvotes | 0 Downvotes

1
VOTE

Anonymous • 14 Jun 2021 13:10 • ✓ ANSWERED

Where are the Cybersecurity requirements stated? is it under ATM or does it fall directly under the HK Security Programme?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:13

With reference to ICAO Annex 17 and Doc 8973, the cybersecurity requirements are stated in the Hong Kong Aviation Security Programme. From ANSP perspective, the cyber security requirements were stemmed from Hong Kong Aviation Security Programme and Doc 9985. HKCAD has a package of security documentations that range from policy objectives down to security measures implementation details.

1 Comment:

Raymond Chan • Allowed on 14 Jun 2021, 15:07 • Hidden

With reference to ICAO Annex 17 and Doc 8973, the cybersecurity requirements are stated in the Hong Kong Aviation Security Programme. From ANSP perspective, the cyber security requirements were stemmed from Hong Kong Aviation Security Programme and Doc 9985. HKCAD has a package of security documentations that range from policy objectives down to security measures implementation details.

0 Upvotes | 0 Downvotes

1
VOTE

Anonymous • 14 Jun 2021 13:11 • ✓ ANSWERED

Please explain is the risk matrix based on security risk level or safety risk level?

1 Answer:



Raymond Chan, Senior Electronics Engineer

Civil Aviation Department (CAD), Hong Kong, China • Submitted on 15 Jun 2021, 12:12

The risk matrix for cyber security security assessment refers to the risk incurred from cyber security threats. The first step is to identify cyber threats, then the second step to analyse and evaluate based on the severity of occurrences and probability. Then categorise and mitigate the identified risk to an acceptable level.

1 Comment:

Raymond Chan • Allowed on 14 Jun 2021, 15:06 • Shown

The risk matrix for cyber security security assessment refers to the risk incurred from cyber security threats. The first step is to identify cyber threats, then the second step to analyse and evaluate based on the severity of occurrences and probability. Then categorise and mitigate the identified risk to an acceptable level.

0 Upvotes | 0 Downvotes



| ICAO

SECURITY & FACILITATION

2021 | THE YEAR OF SECURITY CULTURE

AIR TRAFFIC MANAGEMENT SECURITY AND UPDATES ON ICAO CYBERSECURITY ACTIVITIES

*Mr. Remington Low
ICAO Regional Officer
Aviation Security & Facilitation*





Annex 17 – Security (Amendment 17)

Aviation security Standards and Recommended Practices (SARPs) are mainly contained in Annex 17 - *Security*

Security provisions also in other Annexes (Annex 2, 6, 8, 9, 10, 11, 14, 18) and PANS Docs 4444 and 8168.





National Civil Aviation Security Programme

Annex 17 – *Security* requires States to develop and implement a NCASP:

- addresses the whole range of security activities including, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of response to AUIs
- roles and responsibilities of all agencies, including Air Traffic Services (ATS) Providers, as related to security operations



Relevant SARPs to ATS Providers

- S 3.5: require ATSP ... to establish and implement appropriate security provisions to meet the requirements of the NCASP
- S 4.9.1: identify their critical information and communications technology systems and data ..in accordance with a risk assessment, develop and implement, ...measures to protect them..
- RP 4.9.2: ensure ...measures protect, ...the confidentiality, integrity and availability of the identified critical systems and data. The measures should include ...security by design, supply chain security, .., and the protection ..of any remote access capabilities, ...



ICAO

SECURITY & FACILITATION



ICAO's Work on Cybersecurity

Legal Instruments:

- The Beijing Convention and The Beijing Protocol of 2010

Assembly Resolutions:

- A39-19 and A40-10 Resolutions on Cybersecurity

Standards and Recommended Practices:

- Annex 17 – *Security*: Standard 4.9.1 and Recommended Practice 4.9.2

Guidance Material:

- Procedures for Air Navigation Services – PANS
- Doc 8973 – *Aviation Security Manual*
- Doc 9985 – *ATM Security Manual*
- Aviation Cybersecurity Strategy
- Cybersecurity Action Plan

Training

- Cybersecurity Training Roadmap
- Training Courses





ICAO Guidance Materials

- Air Traffic Management Security Manual (Doc 9985, Restricted)
- PANS
- Aviation Security Manual (Doc 8973, Restricted – 12th edition)
- ICAO global Risk Context Statement (Doc 10108, Restricted – 2nd edition)
- Aviation Cybersecurity Strategy
- Cybersecurity Action Plan





Training

■ Training Courses in the Pipeline:

- ✓ Foundations of Aviation cybersecurity Leadership and Technical Management
 - Developed in Partnership between ICAO and Embry-Riddle Aeronautical University
 - Two Tracks: Leadership & Technical Management
- ✓ Managing Security in ATM
 - Developed in Partnership between ICAO and EuroControl
 - Covers Traditional ATM Security as well as Cyber





Expert Groups within ICAO Addressing Cybersecurity in their Work

■ Secretariat Study Group on Cybersecurity – SSGC (late 2017)

- ✓ Research Sub-Group on Legal Aspects
- ✓ Working Group on Airline and Aerodromes
- ✓ Working Group on Air Navigation Systems
- ✓ Working Group on Cybersecurity for Flight Safety

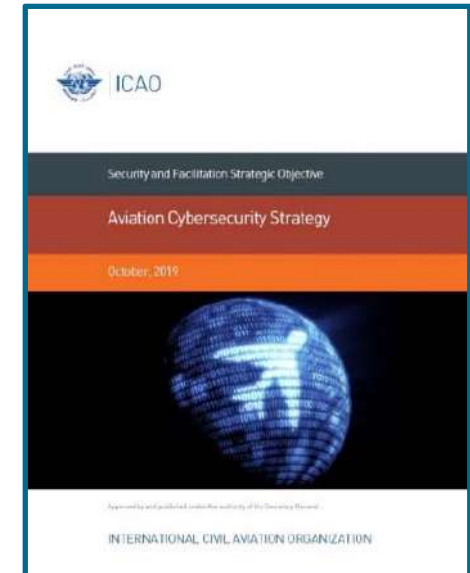
■ Trust Framework Study Group – TFSG

- ✓ Trust Reciprocity Operational Needs Working Group
- ✓ Digital Identity Working Group
- ✓ Global Resilient Aviation Interoperable Network Working Group



Aviation Cybersecurity Strategy

- To protect and ensure continuity of civil aviation operations from cybersecurity threats that affect the safety, security and trust of the air transport system;
- To have States to recognize their obligations under the Convention on International Civil Aviation (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity threats; and
- To allow coordination of cybersecurity measures among State to ensure effective and efficient management of cybersecurity risks.



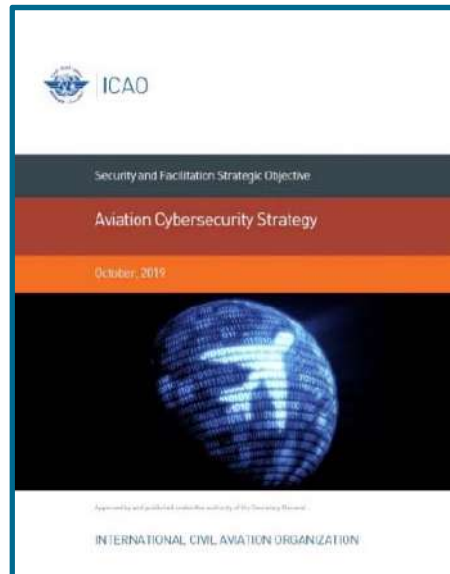


ICAO

SECURITY & FACILITATION

2021 | THE YEAR OF SECURITY CULTURE

Aviation Cybersecurity Strategy



International Cooperation

Governance

Effective Legislation & Regulations

Cybersecurity Policy

Information Sharing

Incident Management & Emergency Planning

Capacity Building, Training, & Cybersecurity Culture



Cybersecurity Action Plan

- 1st edition published in November 2020 issued via State letter 2020/114.
- **Provides the Foundation** for ICAO, States and stakeholders to work together, and proposes a **Series of Principles, Measures, and Actions** to achieve the objectives of the Cybersecurity Strategy's seven pillars.
- **Develops the Seven Pillars** of the Aviation Cybersecurity Strategy into **29 Priority Actions**, which are further broken down into **54 Tasks** to be Implemented by ICAO, States, and Stakeholders



ICAO

SECURITY & FACILITATION



Cybersecurity Action Plan (Example)

Priority Outcome		Pillar 3: DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS					
Priority Actions		• Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and Industry in implementing cybersecurity related provisions; • Ensure that international legal instruments provide appropriate measure for the prevention, timely reaction to, and prosecution of cyber-incidents.					
Actions							
Action #	By	Traceability to the Cybersecurity Strategy	Traceability in Action Plan	Specific Measures/Tasks	Indicators	Maturity	Target
CyAP 3.1	Member States	3.3	8.4	Member States to ratify Beijing instruments.	Number of States having ratified Beijing instruments	Low	ongoing
CyAP 3.2	ICAO	3.3	8.3	Analysis of international air law instruments	Report and update plan	N/A	2020
CyAP 3.3	ICAO and Member States	3.3	8.2	Analysis of existing international and national legislation in the cybersecurity field and identify gaps, including criminal law.	Promote ratification of instruments to incriminate unlawful cyber acts.	Medium	2022 - 2023
CyAP 3.4	ICAO, Member States and Industry	3.3	8.1	Review existing ICAO security standards to identify need for potential cybersecurity updates	Regulatory gap analysis	High	2021
CyAP 3.5	ICAO	3.2	5.4	Create, review and amend guidance material related to implementing cybersecurity requirements	Accepted and agreed cybersecurity guidance material	High	2021-2022



ICAO

SECURITY & FACILITATION



2021 | THE YEAR OF SECURITY CULTURE



ICAO

North American
Central American
and Caribbean
[NACC] Office
Mexico City

South American
[SAM] Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
[WACAF] Office
Dakar

European and
North Atlantic
[EUR/NAT] Office
Paris

Middle East
[MID] Office
Cairo

Eastern and
Southern African
[ESAF] Office
Nairobi

Asia and Pacific
[APAC] Sub-office
Beijing

Asia and Pacific
[APAC] Office
Bangkok



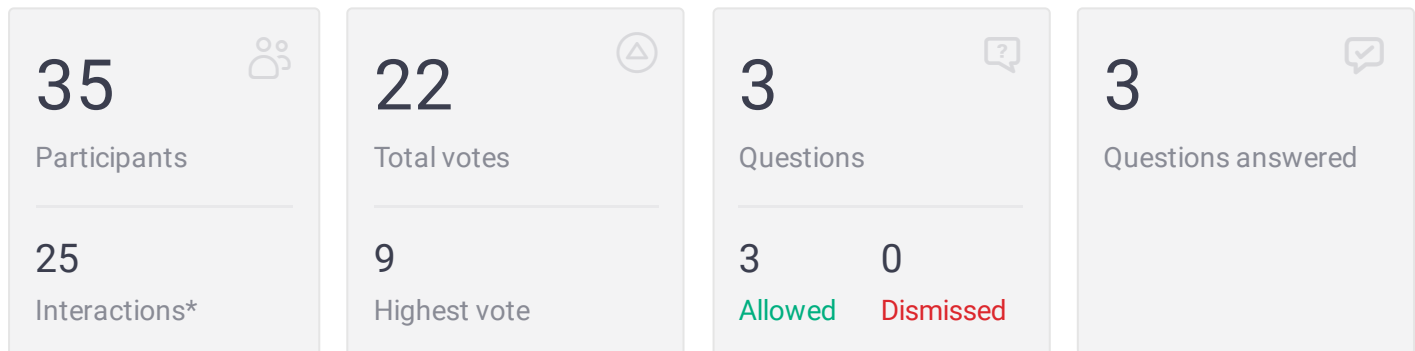
THANK YOU

 Q&A

SP302 – Air Traffic Management Security and Updates on ICAO Cybersecurity Activities

14 Jun 2021, 08:00 - 16:00

by Mr. Remington Low Regional Officer FAL, Asia/Pacific Regional Office, International Civil Aviation Organization (ICAO)



* Interactions include the total number of questions, votes, comments and answer ratings

3 Questions Allowed

9
VOTES
Anonymous • 14 Jun 2021 13:31 • ✓ ANSWERED
The ICAO Guidance Materials looks abundant and comprehensive on global level only. Any of these materials readily available for APAC to refer? Also when will be next training courses by ICAO/partners?

8
VOTES
Anonymous • 14 Jun 2021 09:13 • ✓ ANSWERED
With more Guidance from ICAO thru Secretariat Study Group on Cybersecurity, what kind of measures to ensure these guidance does not fall into the wrong hands while accessible by stakeholders in need?

5
VOTES
Anonymous • 14 Jun 2021 09:12 • ✓ ANSWERED
With the Risk Context Statement you mentioned, the risk of a Cyber-attack is assessed as LOW. Yet, we have come across an increasing number of Cybersecurity crimes. Is this assessment accurate?



A Security Solution for Information Service in SWIM

Tian Yungang
June 2021

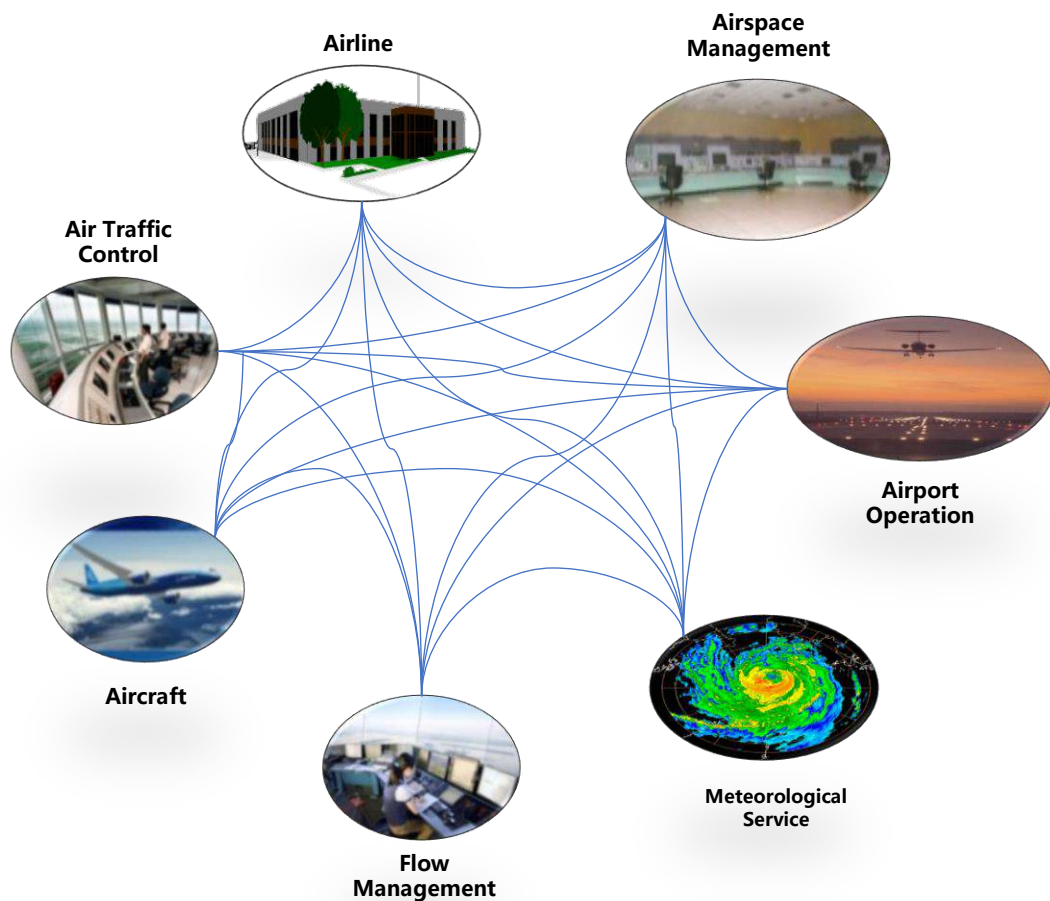
State Key Laboratory of Air Traffic Management System and Technology, China

C contents

- 1 **Introduction**
- 2 Framework
- 3 Solutions
- 4 Conclusion

1. Introduction

Transformation of ATM System



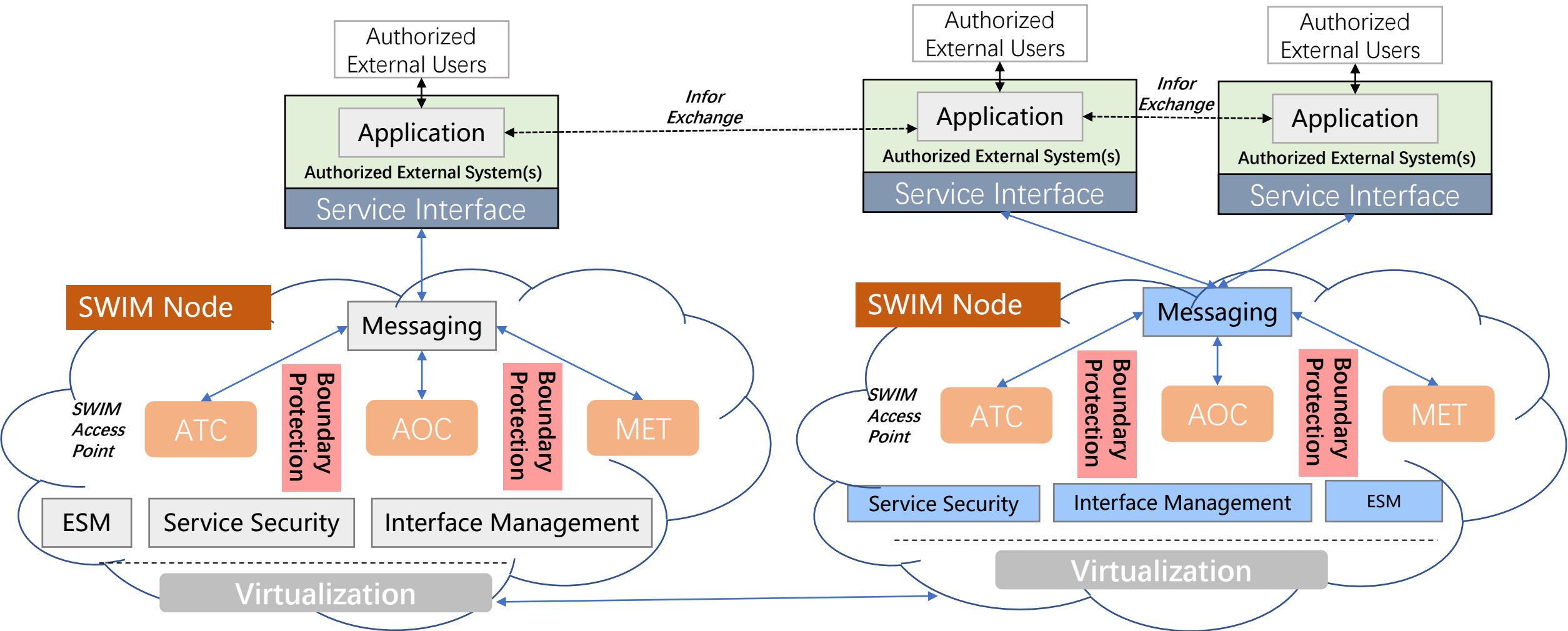
Current ATM system



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: unauthorized 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

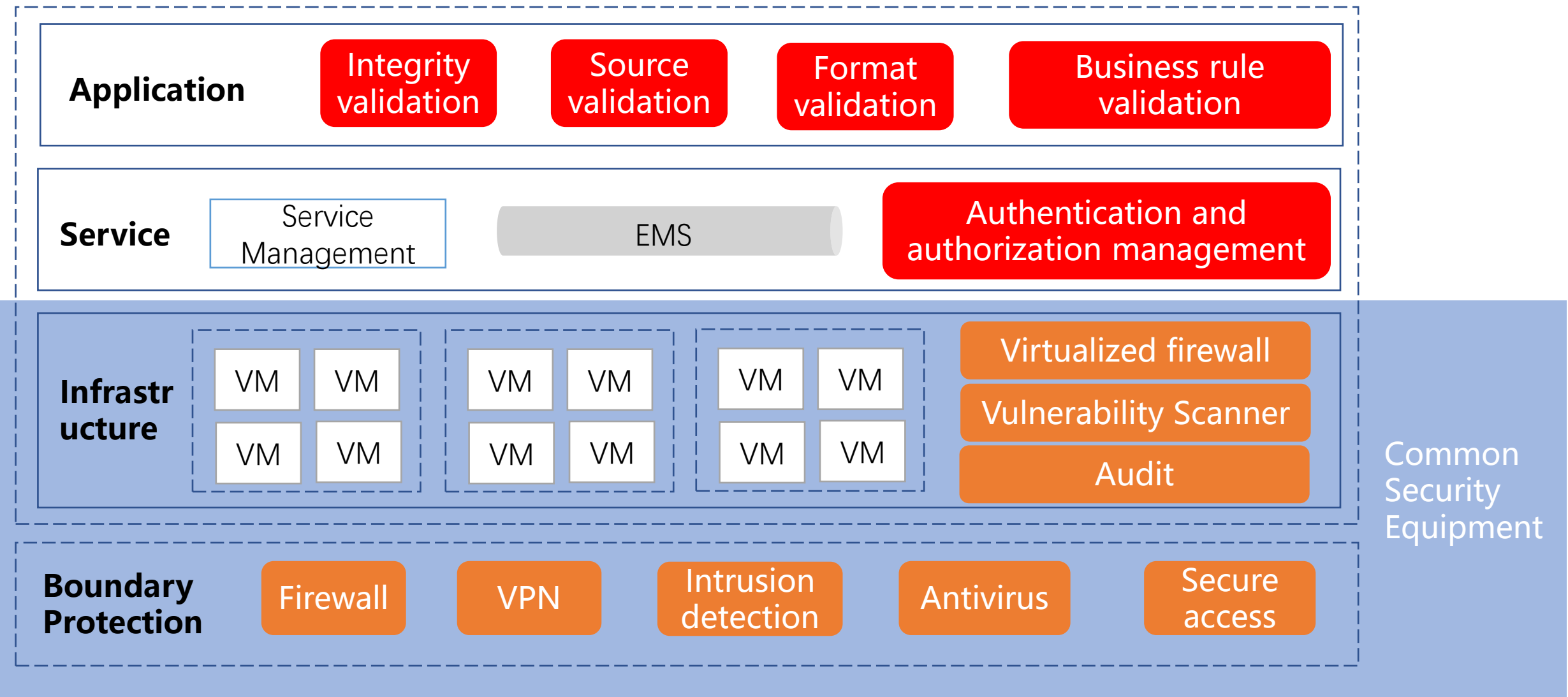
Security Requirements

Application Security	Vulnerability Scanner	Vulnerability Scanner Platform	Code Audit	
	Intrusion Prevention	Web Application Firewall	WebSite Defacement System	
Host Security	Access Control	Access Control	Access Authorization	Resource Management
	Malicious Code	Antivirus Program		
Network Security	Safety Audit	Log Service	Intrusion Prevention	Internet-Based Behavior Management
	Intrusion Prevention	DDOS Protection	Intrusion Prevention	Internet-Based Behavior Management
	Boundary Protection	Firewall	NFV Service Chain	Virtual Firewall
	Access Control	Virtual Host Access Control	Equipment Access Control	Area Access Control
Data Security	Database Audit	Backup and Recovery	Data Encryption	Multi-tenancy Data isolation
Physical Security	Fireproof	Anti-thunder	Electromagnetic potential	Electrical supply

C contents

- 1 Introduction
- 2 **Framework**
- 3 Solutions
- 4 Conclusion

2. Framework

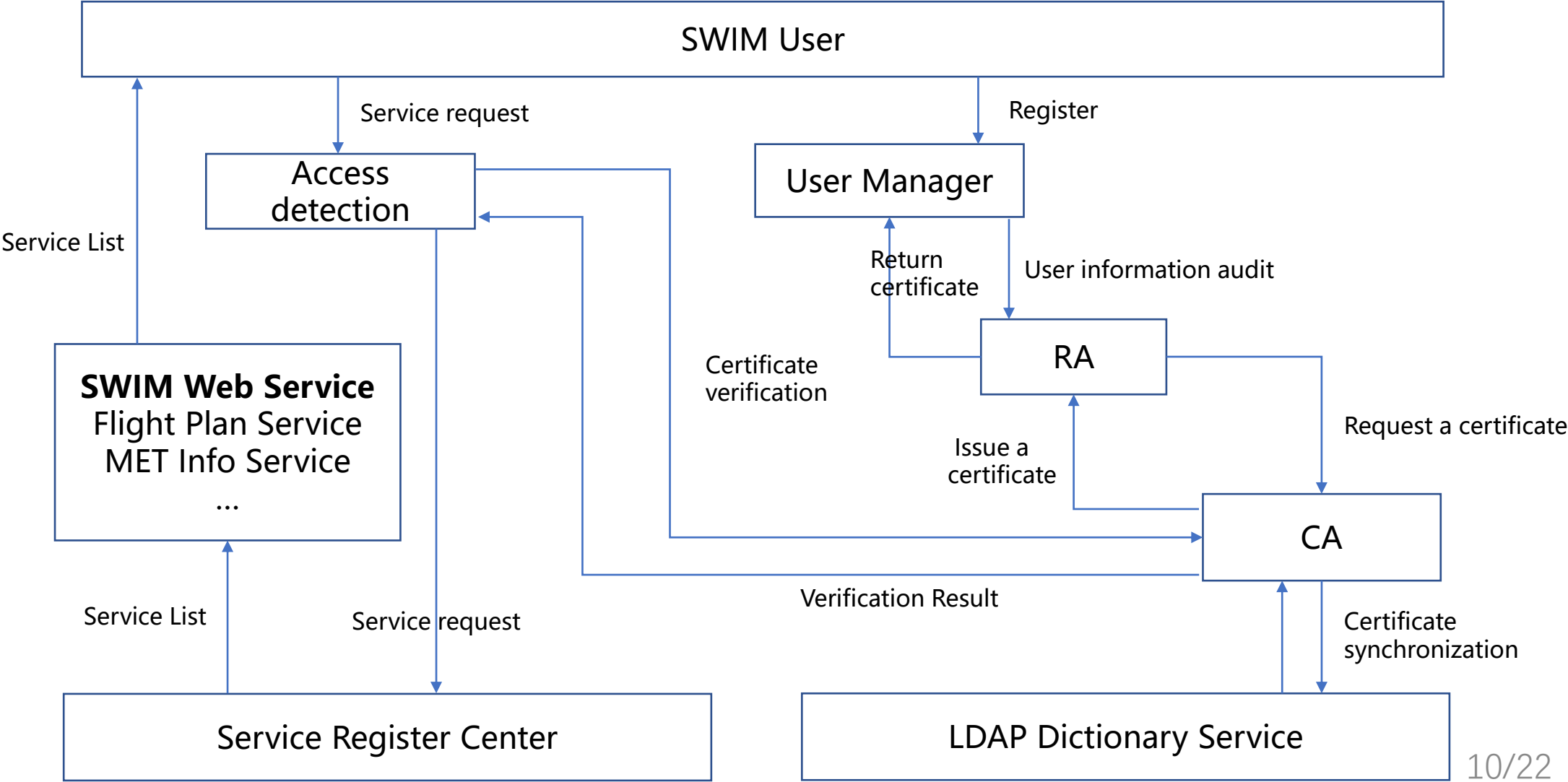


C contents

- 1 Introduction
- 2 Framework
- 3 **Solutions**
- 4 Conclusion

3. Solutions

Authentication



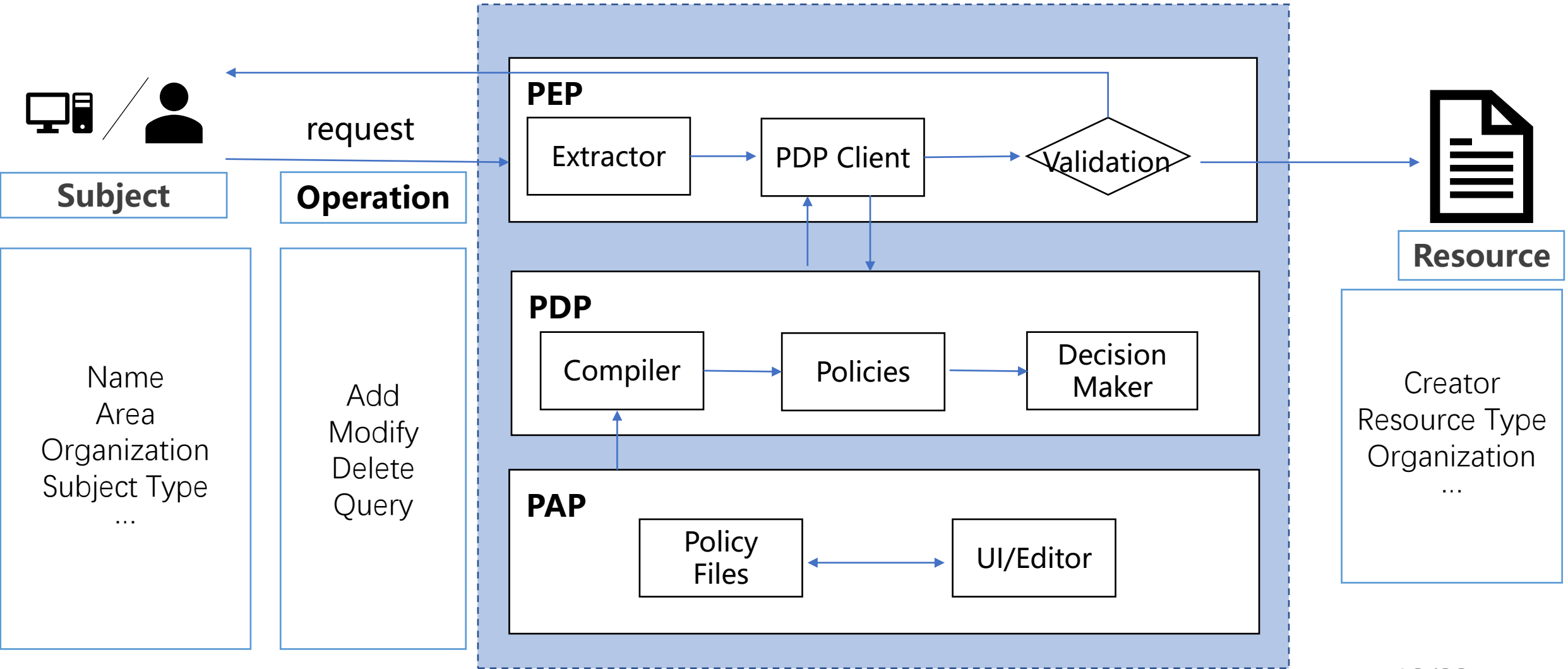
3. Solutions

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

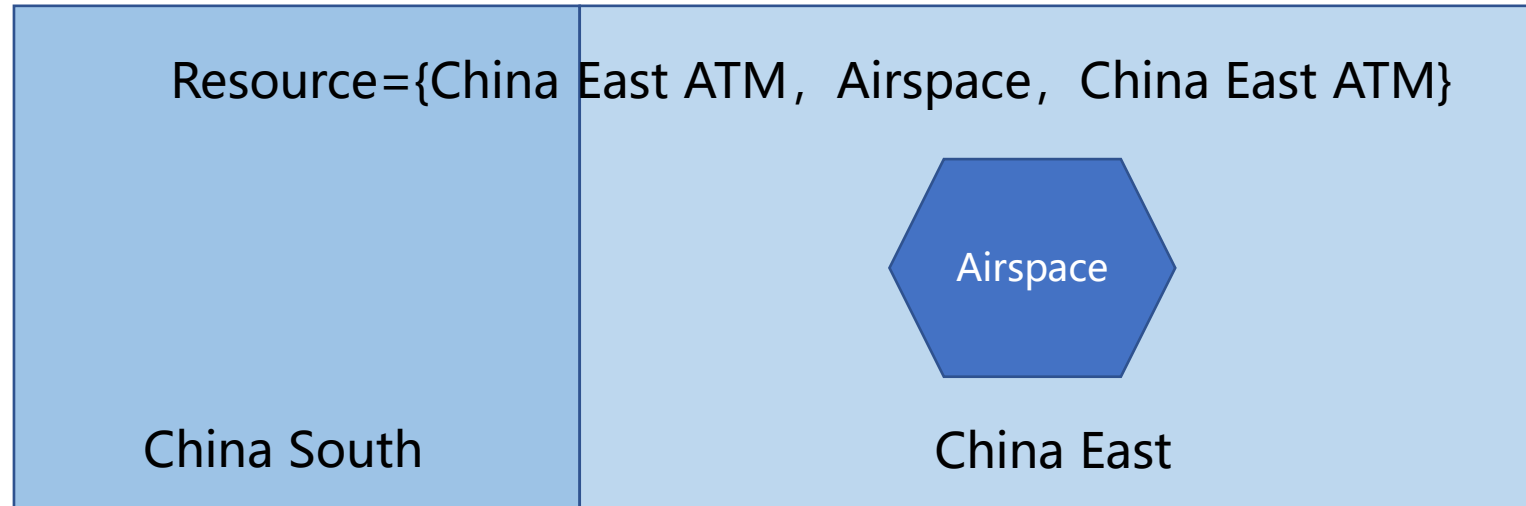
3. Solutions

Authorization—ABAC



3. Solutions

Authorization—ABAC



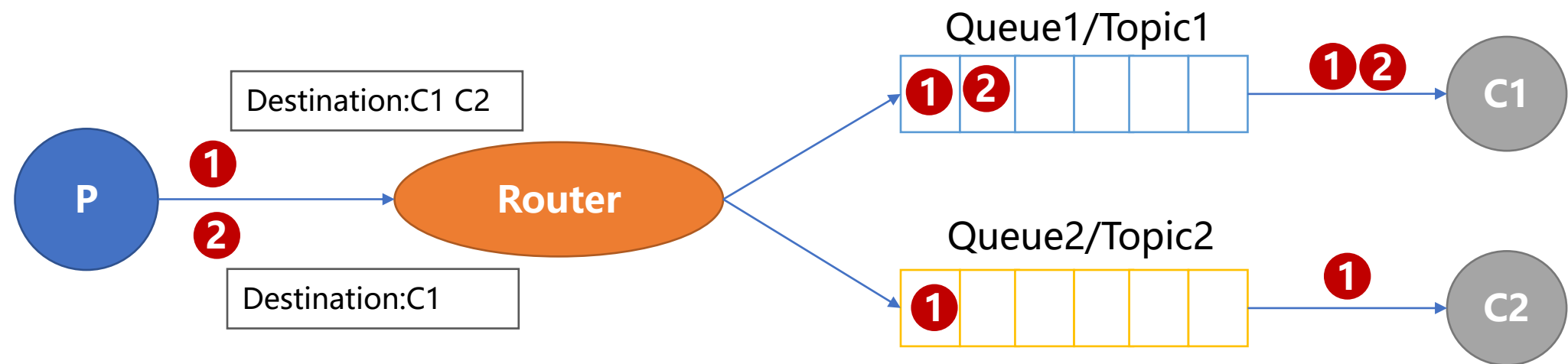
Subject1={China South ATM, **China South**, ATM, ATC System}

Policy={China_East_Area and ATM_Organization and (AMS_SubjectType,ATC System) 1 of 2}

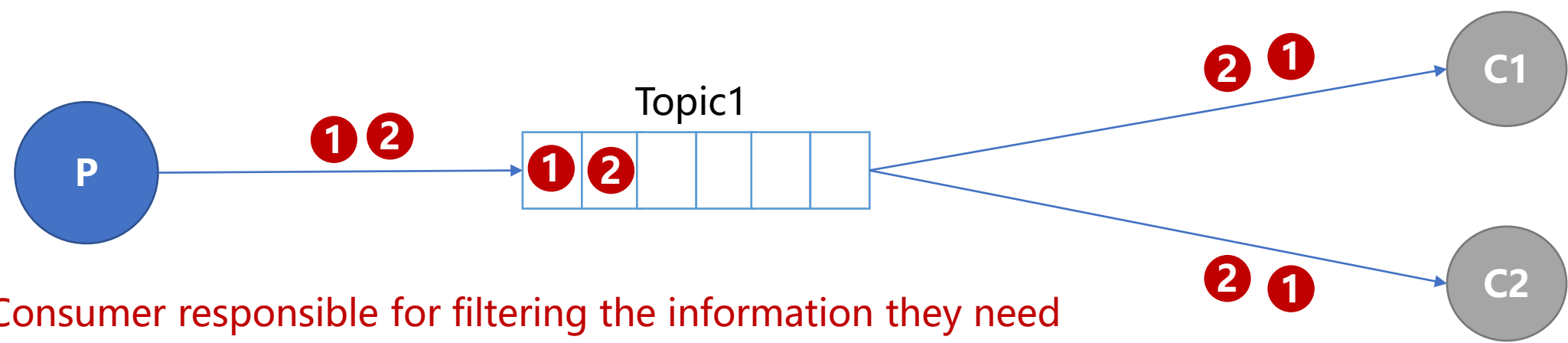
Subject2={China East ATM, China East, ATM, AMS}

3. Solutions

Another way to prevent data diffusion



Provider responsible for controlling the scope of information dissemination

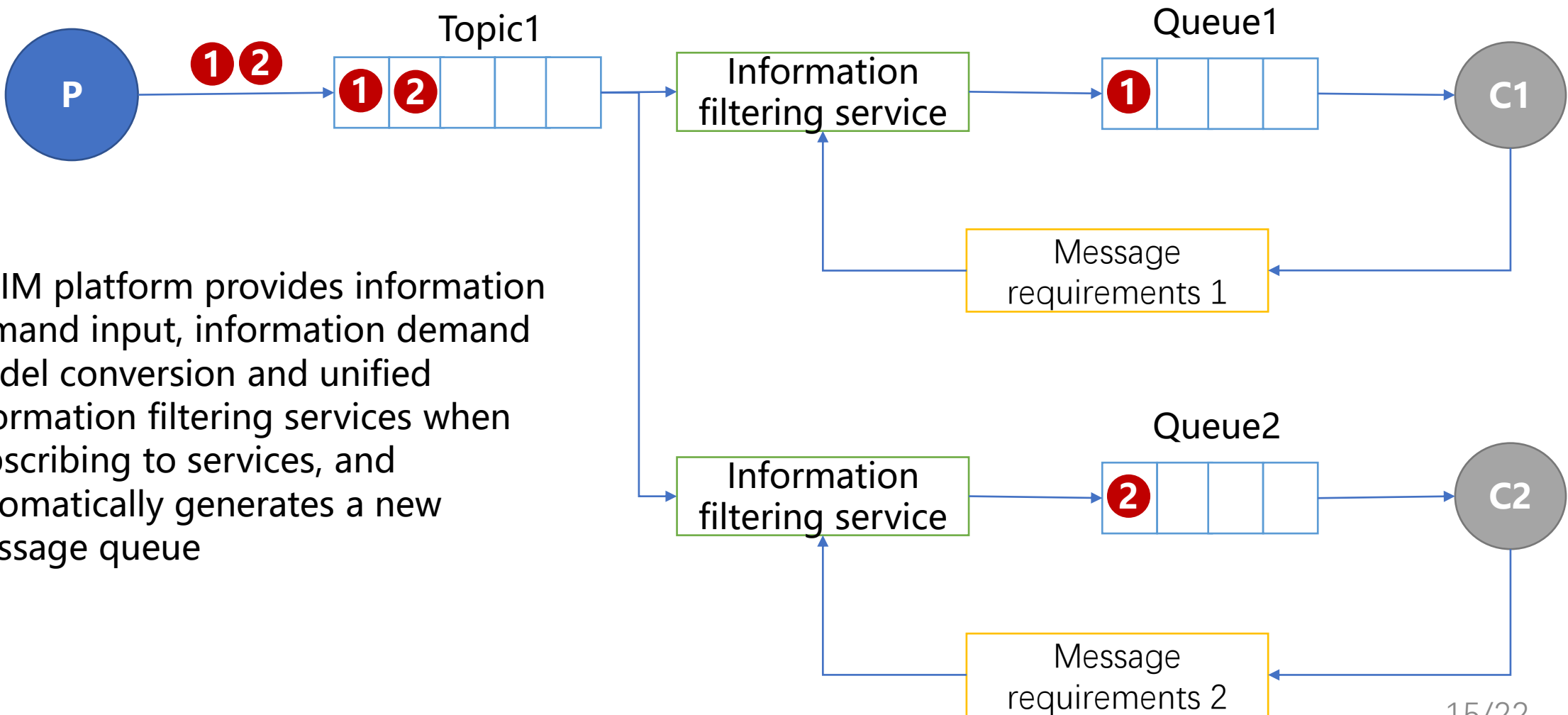


Consumer responsible for filtering the information they need

3. Solutions

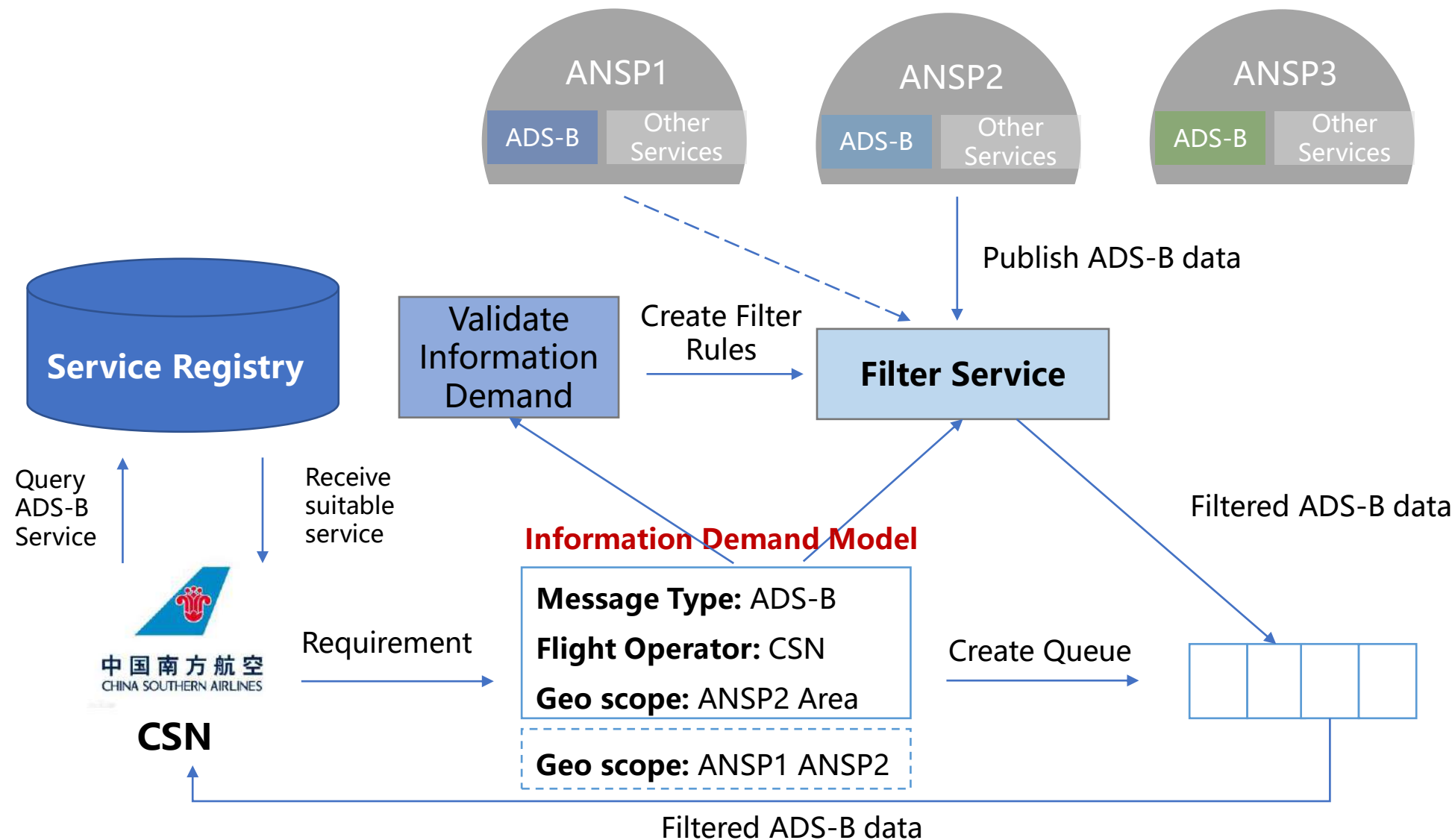
Another way to prevent data diffusion

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

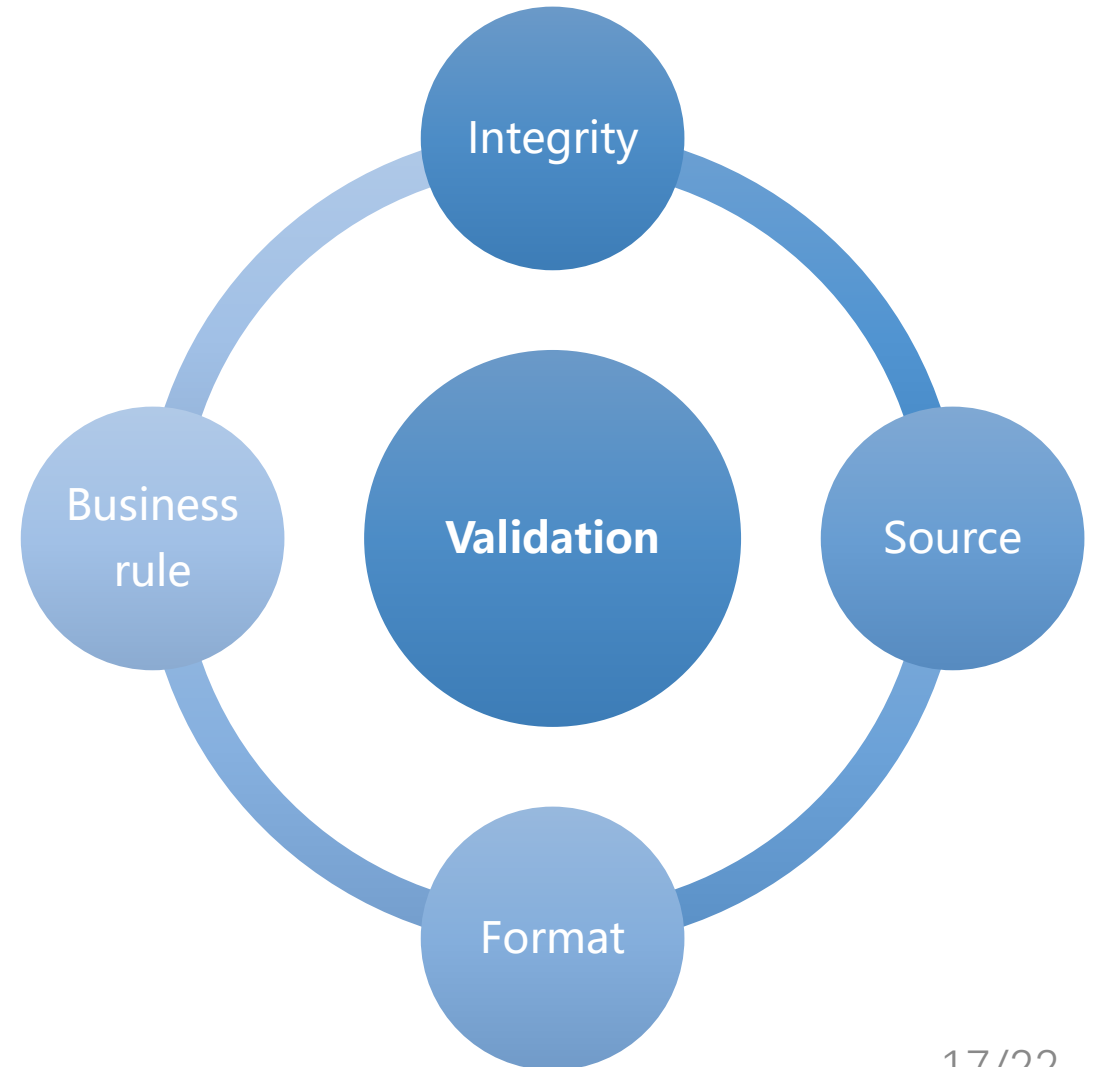
Information validation

Integrity validation: Information tampering validation

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

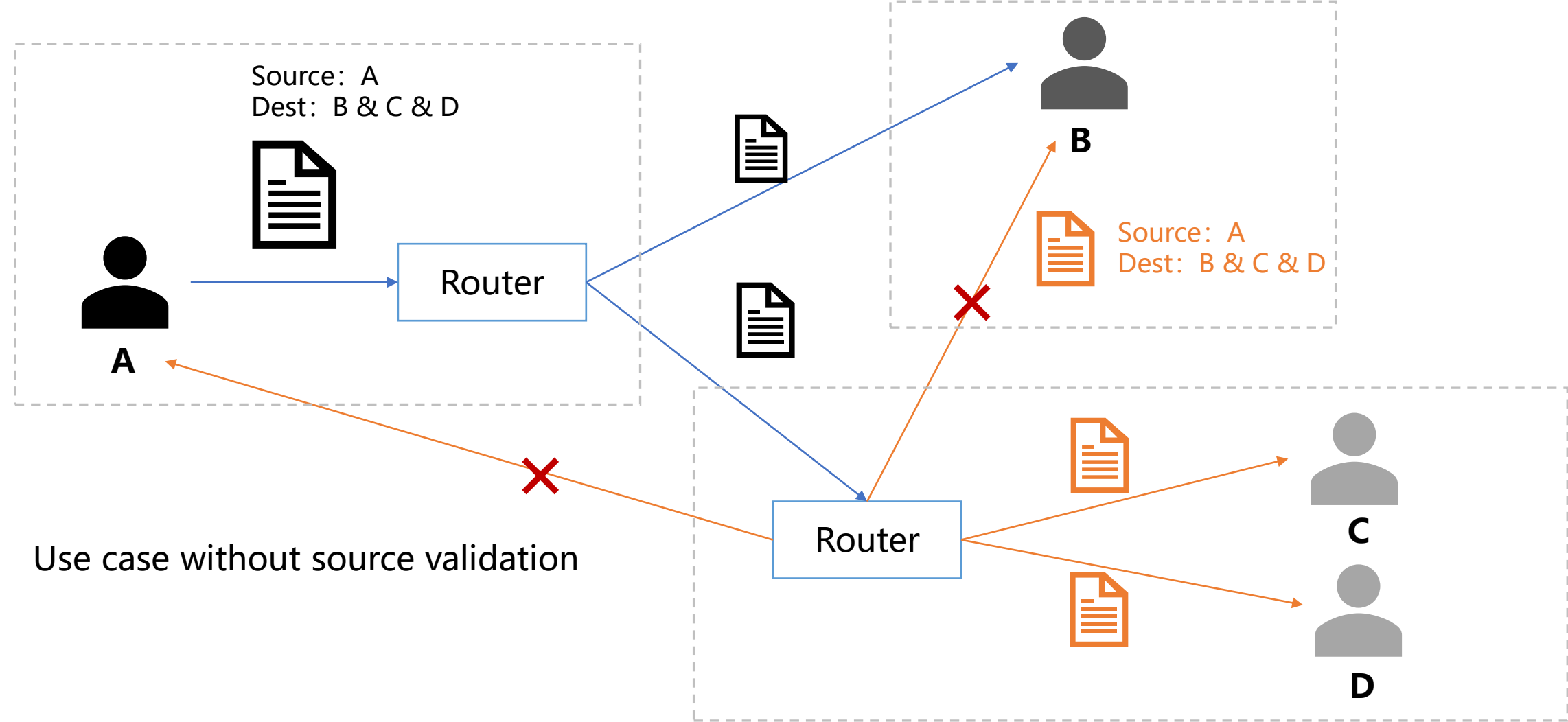
Format validation: Validate the consistency of the information and the information exchange model

Business rule validation: Validate the business logic of the information



3. Solutions

Information validation—Source Validation



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.

C contents

- 1 Introduction
- 2 Framework
- 3 Solutions
- 4 Conclusion

4. Conclusion

Information transmission:
more secure and reliable

Authorization policy:
more flexible





Thank you!

 Q&A

SP303 – A Security Solution for Information Services in SWIM

14 Jun 2021, 08:00 - 16:00

by Mr. Tian Yungang Section Chief, State Key Laboratory of Air Traffic Management System and Technology, China

44 Participants 25 Interactions*	21 Total votes 9 Highest vote	4 Questions 4 Allowed 0 Dismissed	3 Questions answered
--	---	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

4 Questions Allowed

9 VOTES	Anonymous • 14 Jun 2021 10:39 • ✓ ANSWERED There were a number of Authorization schemes introduced - DAC, MAC, RBAC and ABAC. Can you briefly describe what they are and why ABAC is chosen as best for SWIM?
5 VOTES	Anonymous • 14 Jun 2021 13:56 • ✓ ANSWERED Is the solutions introduced here already planned / implemented in SWIM or this is a research result?
4 VOTES	Anonymous • 14 Jun 2021 08:34 • ✓ ANSWERED In your presentation, whether the filter services which can reduce unnecessary sharing has been applied, and how to uniformly describe the different information requirements of different users?
3 VOTES	Anonymous • 14 Jun 2021 14:04 Is the proposed cyber security solution is compatible with existing cyber security systems in Eurocontrol and USA.

Cybersecurity – A vendors perspective

Architecture, Threat, and Mission

Binny Sarien
Security Design Authority Thales Australia



Agenda

Cyber security from a vendors perspective

- Emphasis on deliberate planning (in line with organisational strategy)
- Accurate requirements specification (practical)
- Regional mandates and customer requirements

Key situational awareness aspects

- Architecture and design (peer review is very important)
- Threat modelling (it assists with risk based decision making)
- Critical Vs Non Critical aspects based on mission objectives

A robust cyber security solution

- Balance technical solution and robust procedures (cost benefit analysis)
- Cybersecure-by-design - security aspects present from the beginning
- Ongoing cyber services

Cybersecurity is in Thales DNA

As a **leader in cyber security** and the **worldwide leader in data protection**,
Thales addresses the entire information security lifecycle, the cornerstone of **digital trust**.



5 000

CYBERSECURITY
SPECIALISTS

5

CYBERSECURITY
OPERATIONS
CENTRES



5

DATA
CENTRES



19 of the 20

LARGEST
BANKS

High grade
DATA SECURITY
solutions for

50

COUNTRIES
INCL. NATO COUNTRIES

Operation and
cybersecurity of
critical information
systems for over

130

CUSTOMERS

Cybersecurity
for

9 of the 10

INTERNET
GIANTS



80%

protection of the
world

PAYMENT
TRANSACTIONS

Security for

4 of the 5

OIL
COMPANIES



THALES

Building a future we can all trust

Unique expertise in both ATM & Cybersecurity

The strength of a global vision combining

ATM Operational Technology (OT) and Information Technology (IT) cybersecurity

Expertise & consulting services

- Education & Training
- Risk Assessment
- Roadmapping

Operational Services

- Detection & monitoring
- Security Operations Center
- Rapid Reaction Team

Products & Systems

- Probes & multilevel Gateways
- Analytics platform
- Identity Management System
- Cybersecure architecture

Cyber Security Implementation – Vendor Perspective

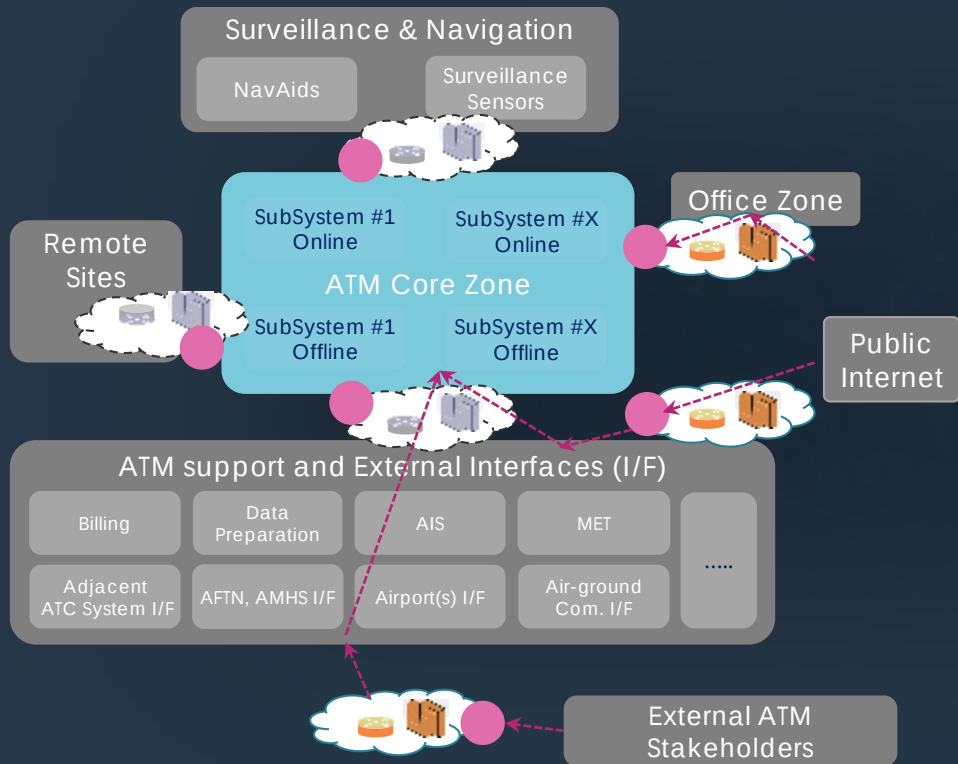
- Vital that cyber security aspects are included in overall strategic objectives of the project
 - Security objectives should be clearly defined and agreed
 - Changing security requirements half-way leads to complications (cost/engineering)
- No Gold standard cyber security template that can be tagged on at the end of the strategic planning
 - Cyber security solutions must be specific to strategy, operating environment and resources available
 - Expectation management from security tools perspective
- Cyber security requirements need to be realistic
 - What are the constraints? budget/skillset/performance
 - Risk based approach (security vs safety)
- ATM infrastructure should comply with the national security authority
 - To be taken into account during requirements gathering
 - Good to establish liaison early and bring them along on the journey

Cyber Security Situational Awareness

Architecture – Network Awareness

- Design discipline and Asset management
- Operational Technology Vs Information Technology
- Routine Vulnerability auditing & management
- System Development Life Cycle
- Applicable security control
- Control testing
- Network Zoning

Zone concept applied to ATM



● Assessment points

Refined with the ANSP considering

- Trusted/Untrusted zones
- Security policies including isolations between zones
- Safety objective

Cyber Security Situational Awareness

■ Threat Awareness

- Threat modelling (internal / external – various techniques attack trees / STRIDE etc)
- Developing indicators of warning
- Liaising with cross-industry and cross-government communities (information sharing)
- Purple Teaming
- Very important for making risk-based decisions.

Asset to Threat mapping - STRIDE model

Firmware	Certificates & keys	Credentials	Network Communication	Configuration	Voice Records	Event logs	Device Resources
Code injection (T)	Replace certificate (TE)	Admin impersonation (SRIE)	Impersonation (SRIE)	Tamper config (T)	Tamper records (T)	Tamper system time (TR)	Debug port abuse (TI)
Reverse engineering (I)	Side channel analysis (I)	Replace credentials (T)	Tamper Package (T)	Impersonation (SI)	Impersonation (SI)	Impersonation (SI)	Eavesdropping busses (I)
Break secure state (TIE)	Corrupt certificate (TD)	Side channel analysis (I)	MITM (RI)	Device Disconnected (TD)	Unauthorised access (IE)	Supress / Erase events (TR)	Abuse resources (DE)
FW corruption (TD)		Corrupt certificate (TIE)		Unauthorised Access (IE)		Unauthorised access (IE)	
Escalation of privilege (IE)							

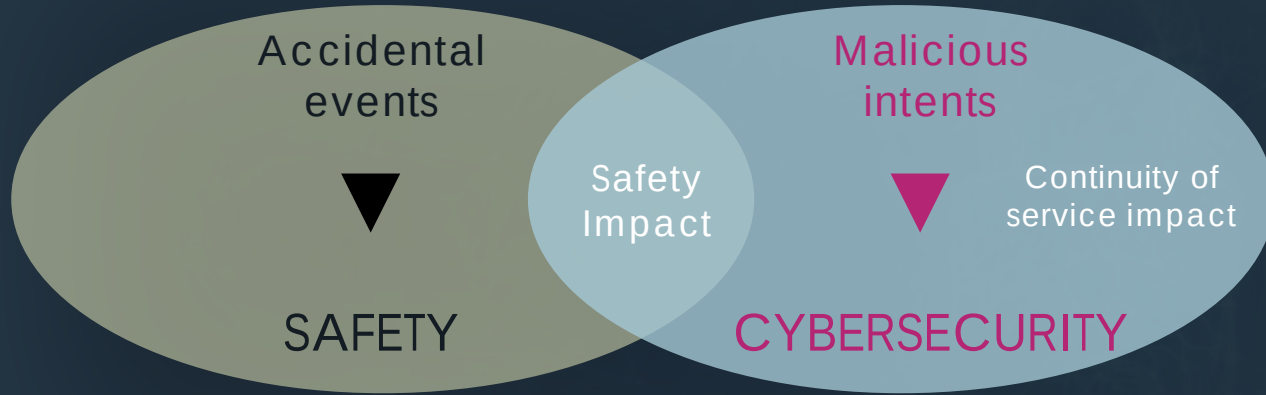
S Spoofing of user identity
 T Tampering
 R Repudiation
 I Information Disclosure
 D Denial of Service
 E Elevation of Privilege

Cyber Security Situational Awareness

Mission Awareness

- Create a common and comprehensive picture of the critical dependencies
- Test security tools with critical functions (safety/performance)
- If cannot block, then ensure that you can record and monitor (appropriate incident response)
- Communication flow in case of an incident

What makes a good solution? Cybersecurity objective



Summary

- **Cyber objectives aligned with organisation, national requirements, and risk appetite.**
- **System of Systems approach**
- **Maintain cyber security situational awareness**
 - Architecture
 - Threat intelligence & management
 - Mission critical objectives
 - Training and contingency planning



Thank you

Binny Sarien

Binny.Sarien@thalesgroup.com.au



Q&A

SP304 – Cybersecurity – A vendors perspective

14 Jun 2021, 08:00 - 16:00

by Mr. Binny Sarien Security Design Authority –Thales Australia – Airspace Mobility Solutions

45 Participants 45 Interactions*	35 Total votes 10 Highest vote	6 Questions 6 Allowed 0 Dismissed	6 Questions answered
--	--	---	--

* Interactions include the total number of questions, votes, comments and answer ratings

6 Questions Allowed

10
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 14:28 • ✓ ANSWERED

Do you view ATM systems more of a operational technology (OT) system or Information Technology (IT) since ATM systems have a lot of IT components such as routers, servers, gateways, datacryptors, etc

1 Answer:



Binny Sarien

Security Design Authority –Thales Australia – Airspace Mobility Solutions • Submitted on 15 Jun 2021, 12:15

ATM systems is consider Information Technology in nature, and operations wise can be categorize as critical systems. Thank you

1 Comment:

Anonymous • Allowed on 14 Jun 2021, 14:45 • Hidden

ATM systems is consider Information Technology in nature, and operations wise can be categorize as critical systems. Thank you

0 Upvotes | 0 Downvotes

8
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 14:39 • ✓ ANSWERED

How does Thales ensure that they are not victims of supply chain attacks and the attacks affect Air Navigations Service Providers (ANSPs). This is because other aviation vendors have become victims

8
VOTES

Zaki (CAA Singapore) • 14 Jun 2021 14:23 • ✓ ANSWERED

How do you manage patch management when systems are operational 24x7 and there is a need to test significantly before deployment?

5
VOTES

Anonymous • 14 Jun 2021 14:26 • ✓ ANSWERED

Given broad implementation experience from Thales, what aspects in cybersecurity implementation APAC lacks or need improvements usually?

1 Answer:



Binny Sarien

Security Design Authority –Thales Australia – Airspace Mobility Solutions • Submitted on 15 Jun 2021, 12:14

Thanks for your question - I would suggest cross industry liaison lead by national government and agencies is the best place to start.

1 Comment:

Binny • Allowed on 14 Jun 2021, 14:57 • Hidden

Thanks for your question - I would suggest cross industry liaison lead by national government and agencies is the best place to start.

0 Upvotes | 0 Downvotes

2
VOTES

Anonymous • 14 Jun 2021 14:41 • ✓ ANSWERED

How to conduct a vulnerability assessment and penetration testing of CNS ATM without sacrificing safety?

1 Answer:



Binny Sarien

Security Design Authority –Thales Australia – Airspace Mobility Solutions • Submitted on 15 Jun 2021, 12:14

We can resort to more passive ways of doing the scan. Also using detection systems works well with safety critical components.

1 Comment:

Binny • Allowed on 14 Jun 2021, 15:03 • Hidden

We can resort to more passive ways of doing the scan. Also using detection systems works well with safety critical components.

0 Upvotes | 0 Downvotes

2
VOTES

Anonymous • 14 Jun 2021 14:41 • ✓ ANSWERED

If you have already implemented any Cybersecurity related sub-systems into ATM systems of any ANSPs?

1 Answer:



Binny Sarien

Security Design Authority –Thales Australia – Airspace Mobility Solutions • Submitted on 15 Jun 2021, 12:14

We have experience of working with Airservices as part of One Sky project.

1 Comment:

Binny • Allowed on 14 Jun 2021, 15:04 • Hidden

We have experience of working with Airservices as part of One Sky project.

0 Upvotes | 0 Downvotes

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

LIST OF PARTICIPANTS

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
1.	AFGHANISTAN (2)			
	1.	Mr. Ahmad Sajjad Safi	Director – CNS Technical Services Afghanistan Civil Aviation Authority	sms.sajjad@yahoo.com ; sajjad.safi@acaa.gov.af ;
	2.	Mr. Zabihullah Marouf	AIS General Manager Afghanistan Civil Aviation Authority (ACAA)	zabihmarouf@gmail.com ;
2.	AUSTRALIA (11)			
	3.	Mr. Jorge Woods	Regulatory Lead, OneSky and Technology Evolution (OSATE) Australia – Civil Aviation Safety Authority (CASA)	jorge.woods@casa.gov.au ;
	4.	Mr. David Cook	Senior Standards Officer Australia – Civil Aviation Safety Authority (CASA)	David.Cook@casa.gov.au ;
	5.	Mr. Kojo Owusu-Akyeampong	Aviation Safety Regulator, OneSky and Technology Evolution (OSATE) Australia – Civil Aviation Safety Authority (CASA)	kojo.owusu-akyeampong@casa.gov.au ;
	6.	Mr. Ken Morris	Aviation Safety Regulator, OneSky and Technology Evolution (OSATE) Australia – Civil Aviation Safety Authority (CASA)	ken.morris@casa.gov.au ;
	7.	Mr. Peter Leigh	Aviation Safety Inspector Australia – Civil Aviation Safety Authority (CASA)	peter.leigh@casa.gov.au ;
	8.	Mr. Jamal Harajli	Aviation Safety Regulator Australia – Civil Aviation Safety Authority (CASA)	jamal.harajli@casa.gov.au ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	9.	Mr. Kev Scrimshaw	Manager Future Airspace Research & Development Program Australia – Civil Aviation Safety Authority (CASA)	Kev.Scrimshaw@casa.gov.au ;
	10.	Mr. Dominic Hides	Assistant Director, Cyber Policy and Workforce Capability Australian Department of Home Affairs, Aviation & Maritime Security Division	dominic.hides@homeaffairs.gov.au ;
	11.	Mr. Tony Kitzelmann	Chief Information Security Officer Airservices Australia	anthony.kitzelmann@airservicesaustralia.com ;
	12.	Mr. Renato Iannella	Lead Data Architect Airservices Australia	renato.iannella@airservicesaustralia.com ;
	13.	Mr. Michael Rossell	Technical Standards Specialist Airservices Australia	michael.rossell@airservicesaustralia.com ;
3.	BANGLADESH (2)			
	14.	Mr. Md Anwar Hossain	Asst NCMC & Aviation Safety Inspector (CNS) Civil Aviation Authority of Bangladesh	ahossaincaab@gmail.com ;
	15.	Mr. Md Shakhaoat Hossain	Air Traffic Controller Civil Aviation Authority of Bangladesh	shakhaoat@gmail.com ;
4.	BHUTAN (2)			
	16.	Mr. Kenzang Tenzin	Senior Communication Supervisor Ministry of Information and Communications Royal Government of Bhutan	tenzinkenjang@gmail.com ;
	17.	Mr. sonam Dorji	Air Traffic Controller Department of Air Transport	sonamd@doat.gov.bt ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
5.	BRUNEI DARUSSALAM (2)			
	18.	Mr. Muhammad Shamrin Abdullah Bundol	Aeronautical Telecommunication Engineer (ATE) Department of Civil Aviation of Brunei Darussalam	shamrin.bundol@dca.gov.bn ;
	19.	Mr. Aimi Tuah	Chief Technician Department of Civil Aviation of Brunei Darussalam	aimi.tuah@dca.gov.bn ;
6.	CHINA (10)			
	20.	Mr. Chen Baogang	Director of General Office ATMB CAAC	hlhlhly@163.com ;
	21.	Mr. Tang Yi	Cybersecurity expert ATMB CAAC	tangyi@atmb.net.cn ;
	22.	Mr. Hou Baoguo	Cybersecurity Expert ATMB CAAC	houbaguo@atmb.net.cn ;
	23.	Mr. Leng Bing	Principal Researcher Southwest Communications Institute (SCI) of China	lengbing@tom.com ;
	24.	Mr. Tian Yungang	Section Chief, State Key Laboratory of Air Traffic Management System and Technology, China	tygbless@126.com ;
	25.	Mr. Li Tianguo	Director State Key Laboratory of Air Traffic Management System and Technology, China	duke60@163.com ;
	26.	Mr. Shen Deren	Engineer Head State Key Laboratory of Air Traffic Management System and Technology, China	shen_dr@qq.com ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	27.	Mr. Tian Jiannan	Engineer State Key Laboratory of Air Traffic Management System and Technology, China	15895871024@163.com ;
	28.	Mr. Zhang Baoli	Engineer State Key Laboratory of Air Traffic Management System and Technology, China	2819835022@qq.com ;
	29.	Mr. Liu Hongyu	Engineer State Key Laboratory of Air Traffic Management System and Technology, China	1662626924@qq.com ;
7.	HONG KONG, CHINA (6)			
	30.	Mr. Raymond Chan	Atg. Senior Electronics Engineer (Project) Civil Aviation Department Hong Kong, China	rwhchan@cad.gov.hk ;
	31.	Ms. Charly Yu	Operations Officer (Avsec Support) Civil Aviation Department Hong Kong, China	ccnyu@cad.gov.hk ;
	32.	Mr. Ronald Lam	Air Traffic Management Standards Officer Civil Aviation Department Hong Kong, China	rkclam@cad.gov.hk ;
	33.	Mr. Francis Fung	IT Manager (Avsec) Civil Aviation Department Hong Kong, China	ftkfung@cad.gov.hk ;
	34.	Mr. Lawrence Law	IT Officer (Cyber Security) Civil Aviation Department Hong Kong, China	Ichlaw@cad.gov.hk ;
	35.	Mr. So Chi-kuen	Scientific Officer Hong Kong Observatory	ckso@hko.gov.hk ;
8.	MACAO, CHINA (6)			

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	36.	Mr. Lo Veng Tong, Freeman	Senior Safety Officer Civil Aviation Authority of Macao, China	freemanlo@aacm.gov.mo ;
	37.	Mr. Pun Sio Kuong, Samson	Safety Officer Civil Aviation Authority of Macao, China	samsonpun@aacm.gov.mo ;
	38.	Mr. Vincent W.P. Tse	Safety Officer Civil Aviation Authority of Macao, China	vincenttse@aacm.gov.mo ;
	39.	Mr. Danny Lam	Head of ATC Service Macau International Airport Co., Ltd.	dannylam@aod.macao-airport.com ;
	40.	Ms. Chan Iok Sam, Kitty	IT & CNS Engineer Macau International Airport Co., Ltd.	kittychan@aod.macao-airport.com ;
	41.	Mr. Ng Huai Chiong, Arnold	IT & CNS Engineer Macau International Airport Co., Ltd.	arnoldng@aod.macao-airport.com ;
9.	FIJI (5)			
	42.	Mr. Sereima Bolanavatu	ANS Inspector (CNS) Civil Aviation Authority of Fiji (CAAF)	sereima.bolanavatu@caaf.org.fj ;
	43.	Mr. Sakiusa	SATO- Quality Assurance & Training Fiji Airport Limited	sakiusav@fijiairports.com.fj ;
	44.	Mr. Shivam Naicker	Senior Aeronautical Technical Officer Fiji Airport Limited	shivamn@fijiairports.com.fj ;
	45.	Mr. Nitesh	System Engineer – ANES Fiji Airport Limited	niteshs@fijiairports.com.fj ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	46.	Mr. Nemani	Aeronautical Technical Officer (Air Navigation Engineering Services) Fiji Airport Limited	nemanic@fijiairports.com.fj ;
10.	INDIA (131)			
	47.	Mr. Umesh Yadav	CNS Inspector Directorate General of Civil Aviation	umeshyadav@aai.aero ;
	48.	Mr. Satya Ranjan Mohapatra	Senior Managaer Airports Authority of India	satya72@aai.aero ;
	49.	Mr. Peddi Srinivas	Joint General Manager (CNS) Airports Authority of India	srinivasp@aai.aero ;
	50.	Mr. Mohan Lal Malvi	Joint General Managaer Airports Authority of India	m_malvi@aai.aero ;
	51.	Mr. Poonam Aggarwal	Asssitant Manager Airports Authority of India	poonam.agg@aai.aero ;
	52.	Mr. Anurag Gupta	AGM CNS Airports Authority of India	a_gupta@aai.aero ;
	53.	Mr. Toogu Naveen Kumar Reddy	Junior Executive (CNS) Airports Authority of India	naveen_k@aai.aero ;
	54.	Mr. Ajay Kumar Kapur	GM (CNS-COM) Airports Authority of India	gmcnscom@aai.aero ; akkapur@aai.aero ;
	55.	Mr. Mohan Lal Malvi	Joint General Managaer Airports Authority of India	m_malvi@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	56.	Mr. Chalasani Babu Rao	Joint General Managaer Airports Authority of India	cbrao@aai.aero ;
	57.	Mr. Suresh Kumar D.	Joint General Managaer Airports Authority of India	dskumar@aai.aero ;
	58.	Mr. Srinivasa Rad G.	Junior Executive (CNS) Airports Authority of India	srinivasa.rg@aai.aero ;
	59.	Mr. Pankaj Kumar Patel	Assistant Manager (CNS) GAGAN Bangalore/Airports Authority of India	pankajpatel@aai.aero ;
	60.	Mr. Dinesh Pal	Senior Engineer Airports Authority of India	dineshpal@aai.aero ;
	61.	Mrs. Indira Abhay Parab	Deputy General Manager (CNS) RHQ, WR, Mumbai Airports Authority of India	indira@aai.aero ;
	62.	Mr. Santosh Kaulagi	Senior Manager (AS) Airports Authority of India	skaulagi@aai.aero ;
	63.	Mr. Pushpendra Kumar Kardam	Senior Manager Airports Authority of India	pkkardam@aai.aero ;
	64.	Mr. Himanshu Verma	Airport in-charge, Solapur Airport Airports Authority of India	aptic_vasl@aai.aero ;
	65.	Mr. Raviraj Lamkane	AM (CNS) Airports Authority of India	cnsicvako@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	66.	Mr. Amritesh Kumar	AM (ELEX) Airports Authority of India	cnsicvajm@aai.aero ;
	67.	Mr. Ashok Kumar Saini	AM (ELEX) Airports Authority of India	aksaini3188@aai.aero ;
	68.	Mr. Agnivesh Singh	Manager (CNS) Airports Authority of India	agnivesh@aai.aero ;
	69.	Mr. Dhaval Jivanlal Vadher	Manager (CNS) Airports Authority of India	dhavalvadher@aai.aero ;
	70.	Mr. Pawan Kumar	Manager (CNS) Airports Authority of India	pawanks@aai.aero ;
	71.	Mr. Vineet Gira	Jt. General Manager (ATSEP) Airports Authority of India	vineetgera@aai.aero ;
	72.	Mr. Gaurav Gupta	Assistant Manager Airports Authority of India	gauravg@aai.aero ;
	73.	Mr. Abhishek Singh	Assistant Manager Airports Authority of India	abhi24@aai.aero ;
	74.	Mr. Vara Prasad Jalli	Assistant General Manager CNS Airports Authority of India	jvprasad@aai.aero ;
	75.	Mr. Madhav Rao Sonkusle	Senior Manager CNS Airports Authority of India	cnsicvasd@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	76.	Mr. Ajay Kumar Das	Senior Manager CNS Airports Authority of India	ajaydas@aai.aero ;
	77.	Mr. Mrinmoy Das	Assistant General Manager CNS Airports Authority of India	mrinmoy.das@aai.aero ;
	78.	Mr. Shivcharan	Manager CNS Airports Authority of India	cnsicvabj@aai.aero ;
	79.	Mr. Ambuj Singh	Assistant Manager(CNS) Kandla Airport Airports Authority of India	ambujsingh92@aai.aero ;
	80.	Mr. Rajesh Bhatt	Assistant Manager (CNS) Airports Authority of India	bhattraajesh@aai.aero ;
	81.	Mr. Tikaram	Assistant Manager(CNS) Airports Authority of India	ram2355@aai.aero ;
	82.	Mr. Anil Kumar Kashyap	DGM (CNS) Airports Authority of India	akashyap@aai.aero ;
	83.	Mrs. Bhoomika Soni	Manager CNS Airports Authority of India	bhoomikas@aai.aero ;
	84.	Mr. Nirmal Bara	AGM (CNS) Airports Authority of India	nirmalbara@aai.aero ;
	85.	Mr. Shri Madhav Rao Sonkusle	Senior Manager CNS Airports Authority of India	cnsicvasd@AAI.AERO ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	86.	Mr. Sumit Kumar Tiwari	Manager CNS Airports Authority of India	sumit04@aai.aero ;
	87.	Mr. Devansh	Junior Executive CNS Airports Authority of India	deve.cns@aai.aero ;
	88.	Mr. Lalit Mohan	Assistant General Manager Airports Authority of India	lalitmohan@aai.aero ;
	89.	Mr. Rakibul Islam	Assistant General Manager (ELEX) Airports Authority of India	rakiaai@gmail.com ;
	90.	Mr. Vinay Sharma	Junior Executive (ELEX) Airports Authority of India	vinay_s@aai.aero ;
	91.	Mr. Sibashis Mondal	Joint General Manager (CNS) Airports Authority of India	smondal@aai.aero ;
	92.	Mr. Suman Ghosh	ATSEP Airports Authority of India	sumanghosh@aai.aero ;
	93.	Mr. Biswajit Ghose	Assistant General Manager (CNS) Airports Authority of India	biswajitg@aai.aero ;
	94.	Mr. Venkatesh Gubbala	Assistant Manager Airports Authority of India	gvenkatesh@aai.aero ;
	95.	Mr. D. Naveen	Manager (CNS) Airports Authority of India	dantoorin@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	96.	Ms. Debashree Sarkar	Assistant Manager (CNS) Airports Authority of India	debashree@aai.aero ;
	97.	Mr. Raja Katta	Assistant Manager Airports Authority of India	katraja@aai.aero ;
	98.	Mr. R. Ganapathi	Senior Manager (CNS) Airports Authority of India	ganapathi82@aai.aero ;
	99.	Mr. Amit Satpathy	Assistant Manager (CNS) Airports Authority of India	amitsatpathy@aai.aero ;
	100.	Mr. Muralidhar Kolli	Assistant General Manager (CNS) Airports Authority of India	kmuralidhar@aai.aero ;
	101.	Mr. Dinesh Gaurawat	Assistant General Manager (ATSEP) Airports Authority of India	dkgaurawat@aai.aero ;
	102.	Mr. Dilawar Hussain	Manager (CNS) Airports Authority of India	dilawar@aai.aero ;
	103.	Mr. Dileep Kumar Singh	AGM CNS Airports Authority of India	dksingh@aai.aero ;
	104.	Mr. Upal Debnath	Senior Manager (CNS) Airports Authority of India	upaldebnath@aai.aero ;
	105.	Mr. Jaynal Abedin	Assistant General Manager (CNS) Airports Authority of India	jayanal@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	106.	Mr. Adarsh Tripathi	Junior Executive Airports Authority of India	adarsh95@aai.aero ;
	107.	Mr. Rajesh Sinha	Joint General Manager Airports Authority of India	rajeshsinha@aai.aero ;
	108.	Mr. Sudipta Kumar Lahiri	AGM (ELEX) Airports Authority of India	sudipta@aai.aero ;
	109.	Mr. Kuntal Bose	Senior Manager (CNS) Airports Authority of India	kuntalbose@aai.aero ;
	110.	Ms. Nitu Maurya	Manager (CNS) Airports Authority of India	nmaurya@aai.aero ;
	111.	Mr. Mukul Kumar	AM (CNS) Airports Authority of India	krmukul92@aai.aero ;
	112.	Mr. Khushiya Singh	Assistant General Manager Airports Authority of India	khushiya@sai.aero ;
	113.	Ms. Vijaya Lakshmi Mahapatra	DGM (CNS) Airports Authority of India	cnsicvejhaai.aero ;
	114.	Mr. Satya Ranjan Mohapatra	Senior Manager (CNS) Airports Authority of India	satya72@aai.aero ;
	115.	Ms. Nisha Kumari	CNS Official Airports Authority of India	nisha_k@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	116.	Mr. Sumitava Karmakar	Manager Airports Authority of India	sumitava@aai.aero ;
	117.	Ms. Archana Paharia	AGM-CNS Airports Authority of India	archanap@aai.aero ;
	118.	Mr. Manjunath Nelli	AGM Airports Authority of India	manjunathnelli@yahoo.com ;
	119.	Mr. Binod Kumar	AGM-CNS Airports Authority of India	binodkumar@aai.aero ;
	120.	Mr. Aji B. R.	Senior Manager CNS Airports Authority of India	aji_br@aai.aero ;
	121.	Mr. Prosenjeet Gon	AM Airports Authority of India	joybaski@aai.aero ;
	122.	Mr. Sudhakar Kumar	Manager (CNS) Airports Authority of India	sudhakar@aai.aero ;
	123.	Mr. Anjul Kumar Khare	AGM CNS Airports Authority of India	anjulkhare@aai.aero ;
	124.	Mr. Ulhas Kulkarni	AGM CNS Airports Authority of India	uskulkarni@aai.aero ;
	125.	Mr. Ravindra R.	Joint General Manger Airports Authority of India	rravindra@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	126.	Mr. Kannan Balasubramaniam	AGM (CNS) Airports Authority of India	kbala@aai.aero ;
	127.	Mr. Pranay Gajbhiye	Assistant Manager Airports Authority of India	pranayg2389@aai.aero ;
	128.	Mr. Alok Raghuwanshi	Joint General Manager (CNS) Airports Authority of India	alok.raghu@aai.aero ;
	129.	Mr. Sumit Biswas	SM (CNS) Airports Authority of India	sumit81@aai.aero ;
	130.	Mr. Anil Kumar S.	Joint General Manager (CNS) Airports Authority of India	anilkumars@aai.aero ;
	131.	Mr. Arun Thomas	Airports Authority of India	arunt@aai.aero ;
	132.	Mr. Pawan Parihar	Joint General Manager (CNS) Airports Authority of India	pawanparihar@aai.aero ;
	133.	Mr. Mani Kant	Assistant General Manager (CNS) Airports Authority of India	kantmani@aai.aero ;
	134.	Mr. Tanniru Kiranmai	CNS O & M Airports Authority of India	Kiranmai421@aai.aero ;
	135.	Mr. Santosh Reddy Kothi	Manager (CNS) Airports Authority of India	santoshreddy@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	136.	Mr. Ravi Kumar R.	Manager (CNS) Airports Authority of India	rrkumar@aai.aero ;
	137.	Mr. Puneet Bhalla	Junior Executive Airports Authority of India	puneet2571993@gmail.com ;
	138.	Ms. Neelima Patel	Junior Executive (CNS) Airports Authority of India	neelima_p@aai.aero ;
	139.	Mr. Devsingh Boda	CNS Official Airports Authority of India	devsinghb@aai.aero ;
	140.	Mr. Vinay Veeravarapu	Assistant Manager Airports Authority of India	vinayveera@aai.aero ;
	141.	Mr. Surya Naik	Manager CNS Airports Authority of India	suryanaik@aai.aero ;
	142.	Mr. Ranga Rao Mahurkar	Joint General Manager (CNS) Airports Authority of India	mahurrao@aai.aero ;
	143.	Mr. Naresh Aiti	CNS Official Airports Authority of India	nareshaiti@aai.aero ;
	144.	Ms. Chitra Verma	Assistant Manager (CNS) Airports Authority of India	chitra112@aai.aero ;
	145.	Mr. Raj Kumar Singh Jadon	Assistant General Manager (CNS) Airports Authority of India	rajkmrjadon@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	146.	Ms. Anjali Gupta	Assistant Manager (CNS) Airports Authority of India	anjaligupta@aai.aero ;
	147.	Mr. Rajashekar C.	Manager (CNS) Airports Authority of India	crajashaker@aai.aero ;
	148.	Mr. Kuntal Bhattacharyya	CNS Official Airports Authority of India	kuntal82@aai.aero ;
	149.	Mr. Gopi Chand Tirupatipati	CNS Official Airports Authority of India	tgcaai13@aai.aero ;
	150.	Mr. Apppala Raju Pedapudi	CNS Official Airports Authority of India	appalaraju@aai.aero ;
	151.	Ms. Padmavathi Narasingu	CNS Official Airports Authority of India	padma07@aai.aero ;
	152.	Ms. Lakshmi Chandala	Joint General Manager Airports Authority of India	lakshmica@aai.aero ;
	153.	Mr. Shailesh Kumar Rathore	Assistant General Manager (CNS) Airports Authority of India	skrathore@aai.aero ;
	154.	Mr. Abhay Kumar	Manager (CNS) Airports Authority of India	abhaykumar@aai.aero ;
	155.	Mr. Saurav Kumar	ATSEP Airports Authority of India	sauravkr@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	156.	Mr. Vihayas Mishra	Manager (CNS) Airports Authority of India	vsmishra@aai.aero ;
	157.	Mr. Gautam Goswami	AGM (ELEX) Airports Authority of India	ggoswami@aai.aero ;
	158.	Mr. Manoj Kumar	Senior Manager (ATSEP) Airports Authority of India	manojaai@gmail.com ;
	159.	Mr. Harinath K.	Manager (CNS) Airports Authority of India	harinathk@aai.aero ;
	160.	Mr. R Mahesh Kumar	Manager (CNS) Airports Authority of India	rmaheshk@aai.aero ;
	161.	Mr. Shankarappa	Deputy General Manager(CNS) Airports Authority of India	shankarappa@aai.aero ;
	162.	Mr. Manoj Kumar Panwar	Senior Manager CNS Airports Authority of India	manojk03@aai.aero ;
	163.	Mr. Ajay Kumar	AGM CNS Airports Authority of India	ajaykumarcom@aai.aero ;
	164.	Mr. Arvind Singh Yadav	Joint General Manager (COM) Airports Authority of India	asyadav@aai.aero ;
	165.	Mr. Partha Prattm Chakraborty	Assistant General Manager (CNS) Airports Authority of India	parthac@aai.aero ;
	166.	Mr. Ashish Bhatnagar	Senior Manager(CNS) Airports Authority of India	abhatnagar@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	167.	Mr. Dipayan Roy	Senior Manager (ELEX) Airports Authority of India	dipayanroy@aai.aero ;
	168.	Mr. Avinash Mani Bhushan Soreng	AGM (CNS) Airports Authority of India	avinash76@aai.aero ;
	169.	Mr. Aditya Kumar	Senior Manager (CNS) Airports Authority of India	adityakumar@aai.aero ;
	170.	Mr. Kurella Akhila Reddy	Junior Executive (CNS) Airports Authority of India	akhila_k@aai.aero ;
	171.	Mr. Sekhar Acharjee	Assistant General Manager (CNS) Kempegowda International Airport Bengaluru	sekhar@aai.aero ;
	172.	Mr. Remya R. Pai	Assistant General Manager (CNS) Airports Authority of India	remyarpai@aai.aero ;
	173.	Mr. Bharat Bhushan Verma	Manager (CNS) Airports Authority of India	bharatverma@aai.aero ;
	174.	Mr. Saurabh Kumar	Manager (CNS) Airports Authority of India	saurabhkumar@aai.aero ;
	175.	Mr. Padamati Yadaiah	Manager (CNS) Airports Authority of India	ypodmati@aai.aero ;
	176.	Mr. Rajesh Kumar Soreng	Sr.Manager (ATSEP) Airports Authority of India	rajeshsoreng@aai.aero ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	177.	Mr. A. Saravanakumar	Joint General Manager (CNS) Airports Authority of India	sarkumar@aai.aero ;
	178.	Mr. Ritesh Kumar Gupta	Joint General Manager (CNS) Airports Authority of India	rk Gupta@aai.aero ;
11.	INDONESIA (4)			
	179.	Ms. Henna Nurdiansari	CNS Inspector Directorate General of Civil Aviation	hennanurdiansari@gmail.com ;
	180.	Ms. Melynessa Sitompul	Airworthiness Engineering Inspector Directorate General of Civil Aviation	Melynessa@gmail.com ;
	181.	Ms. Waya Fadini	Air Navigation Inspector Directorate General of Civil Aviation	waya_fadini@dephub.go.id ;
	182.	Mr. Zainal Arifin Harahap	VP Information Technology AirNav Indonesia	zainal.arifin@airnavindonesia.co.id ;
12.	JAPAN (1)			
	183.	Mr. Manabu Kawamoto	Chief Japan Civil Aviation Bureau	kawamoto-m46vv@mlit.go.jp ;
13.	LAO PDR (1)			
	184.	Mr. Moukphamay Thammavongsa	Aeroanautical Radio System Engineer Lao Air Navigation Services	moukTH@msn.com ;
14.	MALAYSIA (12)			
	185.	Mr. Mohammad Hafiz Salleh	Director Civil Aviation Authority of Malaysia	mhsfiz@dca.gov.my ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	186.	Mr. Sahrol Nizal Ab Rashid	Princiapl Assistant Director Civil Aviation Authority of Malaysia	sahrol@caam.gov.my ;
	187.	Mr. Mohd Hamli Bin Alias	Princiapl Assistant Director Civil Aviation Authority of Malaysia	mohd.hamli@caam.gov.my ;
	188.	Mr. Irman Bin Ridwan	Princiapl Assistant Director Civil Aviation Authority of Malaysia	irman.ridwan@caam.gov.my ;
	189.	Mr. Amiruddin Bin Mustafa	Princiapl Assistant Director Civil Aviation Authority of Malaysia	amirul@caam.gov.my ;
	190.	Mr. Ahmad Syahidan Bin Abu Bakar	Senior Assistant Director Civil Aviation Authority of Malaysia	syahidan@caam.gov.my ;
	191.	Mr. Hafizuddin Bin Mohamed	Assistant Director Civil Aviation Authority of Malaysia	hafizuddin@caam.gov.my ;
	192.	Ms. Norhayati Abdul Rahim	ANS Inspector Civil Aviation Authority of Malaysia	norhayati@caam.gov.my ;
	193.	Mr. Ahmad Khusairi Bin Abdul Wahab	Air Traffic Controller Civil Aviation Authority of Malaysia	khusairi@caam.gov.my ;
	194.	Mr. Anwar Awang Man	Senior Solution Consultant Telekom Malaysia	anod@tm.com.my ;
	195.	Mr. Afiz Abdullah	Senior Solution Consultant Telekom Malaysia	afiz@tm.com.my ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	196.	Mr. Mohd Azmadi Abdullah	Software Engineer SIAGA Laboratories	azmadi@siagalabs.com ;
15.	MONGOLIA (2)			
	197.	Mr. Puntsag Ganbaatar	Senior Inspector Civil Aviation Authority of Mongolia	ganbaatar@mcaa.gov.mn ;
	198.	Mr. Enkhmunkh Enkhbold	Officer Civil Aviation Authority of Mongolia	enkhmunkh.e@mcaa.gov.mn ;
16.	NEPAL (4)			
	199.	Mr. Manohar Rajbhandari	Deputy Director Civil Aviation Authority of Nepal	manohar.rajbhandari@gmail.com ;
	200.	Mr. Suresh Prasad Sah	Deputy Director Civil Aviation Authority of Nepal	suresh@tiairport.com.np ;
	201.	Mr. Pravin Neupane	Deputy Director Civil Aviation Authority of Nepal	pravinneupane@gmail.com ;
	202.	Mr. Upaj Dhakal	Deputy Director Civil Aviation Authority of Nepal	upajdhakal@gmail.com ;
17.	NEW ZEALAND (2)			
	203.	Mr. David Willing	Manager Security Regulation Civil Aviation Authority of New Zealand	David.Willing@caa.govt.nz ;
	204.	Mr. David Wills	Technical Specialist Aeronautical Services Civil Aviation Authority of New Zealand	David.Wills@caa.govt.nz ;
18.	PAKISTAN (6)			

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	205.	Mr. M. Nadeem Akhtar	Senior Joint Director ATS Civil Aviation Authority of Pakistan	NadeemAkhtar@caapakistan.com.pk ;
	206.	Engr. Tariq Hussain	Senior Assistant Director CNS Civil Aviation Authority of Pakistan	Tariq.Hussain@caapakistan.com.pk ;
	207.	Mr. Muhammad Asad Khan Niazi	Joint Director CNS Civil Aviation Authority of Pakistan	innovative.one@hotmail.com ;
	208.	Ms. Hina Mohsin	Assistant Director AVSEC Civil Aviation Authority of Pakistan	Hina.Mohsin@caapakistan.com.pk ;
	209.	Mr. Farhan Ali Qureshi	Assistant Director IT Civil Aviation Authority of Pakistan	farhan.ali@caapakistan.com.pk ;
	210.	Mr. Amjad Hussain	Senior Assistant Director Civil Aviation Authority of Pakistan	amjad.hussain@caapakistan.com.pk ;
19.	PHILIPPINES (21)			
	211.	Mr. Ernesto T. Gagan, Jr.	CNSSO V/ANS Operations Department Civil Aviation Authority of the Philippines	egagtanjr@yahoo.com ;
	212.	Mr. Ferdinand B. Sanchez	Aviation Service Safety Inspector Document Control Officer, IT Officer, AANSOO Civil Aviation Authority of the Philippines	radar.one.ph@gmail.com ;
	213.	Ms. Maria Lyn C. Santamaria	ATMO V/Asst. FIC, MADCC Air Traffic Service Civil Aviation Authority of the Philippines	santamariamarylyn@yhao.com ;
	214.	Mr. Edgar Ricardo S. Tolentino	ATMO IV, Mactan-Davao Approach Cluster Air Traffic Service Civil Aviation Authority of the Philippines	artee1971@gmail.com ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	215.	Ms. Alma Mari M. Dalimot	ATMO IV, Mactan-Davao Approach Cluster Air Traffic Service Civil Aviation Authority of the Philippines	almamari74@yahoo.com ;
	216.	Mr. Roderick S. Basio	ATMO IV, Mactan-Davao Approach Cluster Air Traffic Service Civil Aviation Authority of the Philippines	roderickbasio@yahoo.com ;
	217.	Ms. Mary Grace M. Dalumpines	ATMO III, Manila-Clark Approach Cluster Air Traffic Service Civil Aviation Authority of the Philippines	mgmdalumpines@yahoo.com ;
	218.	Mr. Benjie O. Esber	ATMO III, Manila-Clark Approach Cluster Air Traffic Service Civil Aviation Authority of the Philippines	benjie_esber@yahoo.com ;
	219.	Mr. Roel L. Lorenzo	ATMO III, AIS OPS Air Traffic Service Civil Aviation Authority of the Philippines	roellorenzo@ymail.com ;
	220.	Ms. Ann Marie A. Pasaporte	ATMO III, AIS OPS Air Traffic Service Civil Aviation Authority of the Philippines	annmarie.pasaporte@gmail.com ;
	221.	Ms. MA. Shiela M. Cuesta	ATMO III, PARCC Air Traffic Service Civil Aviation Authority of the Philippines	caaphil.rcc@gmail.com ;
	222.	Ms. Ann Marie A. Pasaporte	Air Traffic Management Officer II Air Traffic Service Civil Aviation Authority of the Philippines	annmarie.pasaporte@gmail.co ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	223.	Mr. Julius Ruel D. Resquir	CNSOO V/Facility-In-Charge, CNS/ATM Air Navigation Service Civil Aviation Authority of the Philippines	jresquir2003@yahoo.com ;
	224.	Mr. Florante B. Bañaria	CNSSO IV Corporate Planning Office Civil Aviation Authority of the Philippines	florante_bb@yahoo.com ;
	225.	Ms. Sofia Paula R. Fulmaran	OIC, MISD Corporate Planning Office Civil Aviation Authority of the Philippines	spfulmaran@caap.gov.ph ;
	226.	Ms. Maria Novelita M. De La Cruz	Data Encoder Controller/Designated CAAP Data Protection Officer MISD, Corporate Planning Office Civil Aviation Authority of the Philippines	mnmdeacruz@caap.gov.ph ;
	227.	Mr. Alan S. Arao Arao	Cybersecurity Consultant MISD, Corporate Planning Office Civil Aviation Authority of the Philippines	cybersecurity@caap.gov.ph ;
	228.	Mr. Armando Navarro	Facility-In-Charge Civil Aviation Authority of the Philippines	rpuxcontrolltower@gmail.com ;
	229.	Mr. Rosemarie Tan	CNS/MET Planning Officer Air Navigation Service Civil Aviation Authority of the Philippines	atmcontplan@gmail.com ;
	230.	Mr. Leo Mantilla	Air Traffic Controller Civil Aviation Authority of the Philippines	leoman711925@gmail.com ;
	231.	Mr. Agustin Cabrera	Aviation Services Safety Inspector Civil Aviation Authority of the Philippines	avcabrera88@yahoo.com ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
20.	REPUBLIC OF KOREA (13)			
	232.	Mr. Huho Ha	Deputy Director Office of Civil Aviation	hoo_ha@korea.kr ;
	233.	Ms. Mia Ji	Assistant Director Ministry of Land, Infrastructure and Transport of the Republic of Korea (MOLIT)	miaji@korea.kr ;
	234.	Ms. Yu-jin Cha	Assistant Director Ministry of Land, Infrastructure and Transport of the Republic of Korea (MOLIT)	yjcha8@korea.kr ;
	235.	Mr. Shin Mingu	Ministry of Land, Infrastructure and Transport of the Republic of Korea	starshin91@korea.kr ;
	236.	Mr. YoungJong Lee	Air Traffic Controller Ministry of Land,Transport and Maritime Affairs	atc100@korea.kr ;
	237.	Mr. Jung Yoon Lee	Civilian Officer Ministry of Land, Infrastructure and Transport of the Republic of Korea (MOLIT)	liyun@korea.kr ;
	238.	Mr. Sang-Hyeon Lee	Public Officer Incheon Air Traffic Control Regional Office	shlee9@korea.kr ;
	239.	Mr. Donglyul Kim	Manager Incheon International Airport Corporation (IIAC)	dongryulkim@airport.kr ;
	240.	Mr. Sung Hwan Kang	AIS Division Incheon Air Traffic Control Regional Office	zeushwan@korea.kr ;
	241.	Mr. Jaekwan Ahn	Deputy Director Incheon International Airport Corporation (IIAC)	jaekwan_ahn@airport.kr ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	242.	Mr. Haneul Park	Assistant Incheon International Airport Corporation (IIAC)	h4neul.park@airport.kr ;
	243.	Mr. Jeonggeun Lee	Official Korean Airport Corporation	netboy@airport.co.kr ;
	244.	Mr. Seonggeun Park	Official Korean Airport Corporation	sg1227@airport.co.kr ;
21.	SINGAPORE (6)			
	245.	Mr. Chua Kim Hee	Deputy Director (CNS) Civil Aviation Authority of Singapore	CHUA_Kim_Hee@caas.gov.sg ;
	246.	Mr. Wee Sin Ho	Deputy Director Civil Aviation Authority of Singapore	Ho_wee_sin@caas.gov.sg ;
	247.	Mr. Wei Chun Gan	Senior Engineer Civil Aviation Authority of Singapore	gan_wei_chun@caas.gov.sg ;
	248.	Mr. De Wei Lim	Senior Air Traffic Control Manager (ATM Integration and Collaboration) Civil Aviation Authority of Singapore	lim_de_wei@caas.gov.sg ;
	249.	Mr. Mohammad Zaki Ariffin	Senior Manager (Cybersecurity) Civil Aviation Authority of Singapore	mohd_zaki_ariffin@caas.gov.sg ;
	250.	Ms. Lucy Tan	Principal Engineer (ANS Cybersecurity) Civil Aviation Authority of Singapore	lucy_tan@caas.gov.sg ;
22.	SRI LANKA (9)			
	251.	Mr. Kalum Prasanna	Director Air Navigation Services Civil Aviation Authority of Sri Lanka	dans@caa.lk ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	252.	Ms. Thilini Herath	Senior Civil Aviation Inspector – ATMSP Civil Aviation Authority of Sri Lanka	scaiatmsp@caa.lk ;
	253.	Mr. Thilina Warnasinghe	Senior Civil Aviation Inspector ATM-OPS Civil Aviation Authority of Sri Lanka	thilina_prasad@yahoo.com ;
	254.	Mr. Dhanula Jayarathna	Civil Aviation Inspector – AIS Civil Aviation Authority of Sri Lanka	caiais1@caa.lk ;
	255.	Mr. Nagalingam Navajeevan	Civil Aviation Inspector – ATSEP Civil Aviation Authority of Sri Lanka	caiatmsp@caa.lk ;
	256.	Mr. Chamara Liyanage	Senior Electronics Engineer Airport and Aviation Services (Sri Lanka) Ltd.	chamara.eane@airport.lk ;
	257.	Ms. Mihiri Yapa Pahalage	Senior Electronics Engineer Airport and Aviation Services (Sri Lanka) Ltd.	mihi.yapa@gmail.com ;
	258.	Mr. Upula Perera	Assistant Engineer Airport and Aviation Services (Sri Lanka) Ltd.	upula.eane@airport.lk ;
	259.	Ms. Nishani Cooray	Manager AIS Airport and Aviation Services (Sri Lanka) Ltd.	nishani_cooray@yahoo.com ;
23.	TIMOR – LESTE (1)			
	260.	Mr. Armando Da Silva	Director/NCMC Civil Aviation Authority of Timor-Leste	armando_dasilva@yahoo.com ;
24.	THAILAND (6)			
	261.	Mr. Takdanai Wuthisen	CNS Officer Civil Aviation Authority of Thailand	takdanai.w@caat.or.th ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	262.	Mr. Nattaporn Pornsawat	Officer Civil Aviation Authority of Thailand	nattaporn.p@caat.or.th ;
	263.	Mr. Wanchalearm Petsuwan	Computer Technical Officer Thai Meteorological Department	wpetsuwan@hotmail.com ;
	264.	Mr. Sutham Sujaritthammakun	Executive Air Traffic System Engineer Aeronautical Radio of Thailand Ltd.	sutham.su@aerothai.co.th ; sutham.tae@gmail.com ;
	265.	Mr. Pichate Soontrawong	Engineering Manager Aeronautical Radio of Thailand Ltd.	pichate.so@aerothai.co.th ;
	266.	Mr. Yorkiat Chaiiad	Engineering Manager Aeronautical Radio of Thailand Ltd.	yorkiat@aerothai.co.th ;
25.	USA (16)			
	267.	Mr. Ricky Chitwood	Aviation Safety Inspector - Air Carrier Operations Flight Standards – Avionics Maintenance Branch Federal Aviation Administration	ricky.chitwood@faa.gov ;
	268.	Mr. Robert Segers	Enterprise Safety & Information Security Division NextGen ISS Architect Federal Aviation Administration	robert.segers@faa.gov ;
	269.	Mr. Christopher D. Mills	Integration, Outreach and Planning Team Air Traffic Organization Cybersecurity Group – Contract Support Federal Aviation Administration	christopher.d-ctr.mills@faa.gov ;
	270.	Mr. Michael Watkins	Senior Air Traffic Representative, Asia Pacific Air Traffic Organization, System Operations Federal Aviation Administration	michael.w.watkins@faa.gov ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	271.	Ms. Marie B. Manalo	Asia-Pacific Program Analyst Air Traffic Organization International Office, Asia Pacific Region Federal Aviation Administration	marie.b.manalo@faa.gov ;
	272.	Mr. Sam El-Zoobi	Program Officer, Asia Pacific Group Air Traffic Organization International Office, Mission Support Federal Aviation Administration	sam.el-zoobi@faa.gov ;
	273.	Ms. Stephanie Braxton	Computer Specialist, Integration, Outreach and Planning Team Air Traffic Organization Cybersecurity Group Federal Aviation Administration	stephanie.m.braxton@faa.gov ;
	274.	Mr. Ted Rush :	Enterprise Cyber Architecture Design & Solutions Manager Air Traffic Organization Cybersecurity Group Federal Aviation Administration	ted.rush@faa.gov ;
	275.	Mr. Hector Morales	Manager, Cyber Engineering Team Federal Aviation Administration	hector.morales@faa.gov ;
	276.	Mr. Joseph S. Baden	Foreign Affairs Specialist Aviation Safety International Federal Aviation Administration	Joseph.Baden@faa.gov ;
	277.	Ms. Barbara Skawinska	Foreign Affairs Specialist Aviation Safety International, APAC Region	Barbara.skawinska@faa.gov ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	278.	Mr. Roderick Degrate	Air Traffic Oversight Inspector, NAS Services Operations Branch Air Traffic Oversight Services Federal Aviation Administration	Roderick.degrate@faa.gov ;
	279.	Mr. Jeffrey A. Bruck	Air Traffic Safety Inspector, Aeronautical Information Standards Branch Air Traffic Oversight Services Federal Aviation Administration	jeffrey.a.bruck@faa.gov ;
	280.	Mr. Nigel Simmons	Senior Principal Engineer (FAA Support) FAA International Telecommunication Service Federal Aviation Administration	Nigel.CTR.Simmons@faa.gov ;
	281.	Mr. Hoang Tran	International Telecommunications Lead Federal Aviation Administration	hoang.tran@faa.gov ;
	282.	Mr. Devinder M. Arora	Civil Aviation Specialsit Federal Aviation Administration Federal Aviation Administration	devinder.arora@faa.gov ;
26.	VIET NAM (1)			
	283.	Mr. Nguyen Hong Hiep	IT Specialist Viet Nam Air Traffic Management Corporation	nguyenhonghiepbk@vatm.vn ;
27.	AAPA (1)			
	284.	Mr. Desmond Yeoh	Manager - Technical Affairs Association of Asia Pacific Airlines (AAPA)	dyeoh@aapa.org.my ;
28.	CANSO (2)			
	285.	Mr. Hai Eng Chiang	Director Asia Pacific Affairs Civil Air Navigation Services Organization	hai.eng.chiang@canso.org ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	286.	Mr. Shayne Campbell	CANSO Safety Programme Manager Civil Air Navigation Services Organization	Shayne.Campbell@CANSO.org ;
29.	IATA (6)			
	287.	Mr. John Moore	Assistant Director- Safety and Flight Operations- ASPAC International Air Transport Association (IATA)	moorej@iata.org ;
	288.	Mr. Jose Frnandez	Manager Audit Stadards International Air Transport Association (IATA)	fernandezj@iata.org ;
	289.	Mr. Yoshiki Imawaka	Executive Advisor All Nippon Airways (ANA)	y.imawaka@ana.co.jp ;
	290.	Ms. Elle Lee	Senior Dispatcher China Airlines	ellelee2010@163.com ;
	291.	Mr. Jung Sik Kim	Chief Specialist CNS/ATM Korean Air	jungsikkim@koreanair.com ;
	292.	Mr.Cheng Yeow Tan	Manager On-Time Performance Singapore Airlines	chengyeow tan@singaporeair.com.sg ;
30.	ICANN (2)			
	293.	Mr. Champika Wijayatunga	Technical Engagement Manager – Asia Pacific Internet Corporation for Assigned Names and Numbers (ICANN)	champika.wijayatunga@icann.org ;
	294.	Mr. Jian-Chuan Zhang	Head of China Internet Corporation for Assigned Names and Numbers (ICANN)	jianchuan.zhang@icann.org ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
31.	IFALPA (9)			
	295.	Captain Amornvaj Mansumitchai	Deputy President International Federation of Air Line Pilots' Associations (IFALPA)	amornvaj@ifalpa.org ;
	296.	Captain Ishtiaque Hossain	EVP APAC International Federation of Air Line Pilots' Associations (IFALPA)	ishtiaquehossain@ifalpa.org ;
	297.	Captain Max Matsumoto	RVP NOP International Federation of Air Line Pilots' Associations (IFALPA)	max.matsumoto@alpajapan.org ;
	298.	Captain David Griffin	RVP SOP International Federation of Air Line Pilots' Associations (IFALPA)	david@griffin.org.nz ;
	299.	Captain Farouk Zahir	RVP Asia/East International Federation of Air Line Pilots' Associations (IFALPA)	faroukzahir@gmail.com ;
	300.	Captain Bhudhibhuntu	International Federation of Air Line Pilots' Associations (IFALPA)	bhudhibhuntu@gmail.com ;
	301.	Captain Dr. Kanit Atisuthapoch	International Federation of Air Line Pilots' Associations (IFALPA)	kanitatstp@gmail.com ;
	302.	SFO Sivanit Ratanadib	International Federation of Air Line Pilots' Associations (IFALPA)	pastrium@gmail.com ;
	303.	Captain Luke Cutler	Q330 First Officer/AIPA Security Officer International Federation of Air Line Pilots' Associations (IFALPA)	lukecutla@hotmail.com ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
32.	IFATCA (1)			
	304.	Mr. Anthony Ang	Executive Vice- President Asia Pacific Region International Federation of Air Traffic Controllers’ Associations (IFATCA)	anthony.ang@ifatca.org ;
33.	SPONSOR - NOKIA (4)			
	305.	Mr. Mervyn Harris	Global Head, Air Traffic Management NOKIA	mervyn.harris@nokia.com ;
	306.	Mr. Sawanjit Singh	Director Aviation Business Development NOKIA	sawanjit.singh@nokia.com ;
	307.	Mr. Harald Illias	Head of Sales Transportation APAC & Americas, Nokia Enterprise NOKIA	harald.illias@nokia.com ;
	308.	Mr. Fai Lam	Head of Transportation Marketing NOKIA	fai.lam@nokia.com ;
34.	SPONSOR - THALES (7)			
	309.	Mr. Binney Sarien	Security Design Authority Thales Australia	binny.sarien@thalesgroup.com.au ;
	310.	Mr. Andrew Nabarro	Business Development Manager Thales Australia	Andrew.nabarro@thalesgroup.com.au ;
	311.	Mr. Roland Huber	Lead Solution Design Authority - Thales Australia	roland.huber@thalesgroup.com.au ;
	312.	Mr. Philip Lorenz	Product Design Architect Thales Australia	Philip.lorenz@thalesgroup.com.au ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	313.	Mr. Ketan Gautam	Cybersecurity Architect Thales Australia	Ketan.Gautam@thalesgroup.com.au ;
	314.	Mr. Lionnel Wonneberger	Director Business Development Thales Australia	lionnel.wonneberger@thalesgroup.com.au ;
	315.	Mr. Philippe Jasslin	Cybersecurity Expert Thales Australia	philippe.jasselin@thalesgroup.com ;
35.	ICAO (13)			
	316.	Ms. Olga de Frutos Martin	Technical Officer, Air Navigation Systems International Civil Aviation Organization Headquarters	Odefrutos@icao.int ;
	317.	Mr. Michael Goodfellow	Technical Officer, Global Interoperable Systems International Civil Aviation Organization Headquarters	MGoodfellow@icao.int ;
	318.	Mr. Raphael Guillet	Chief of the APAC Regional Sub-Office International Civil Aviation Organization Asia and Pacific Office	rguillet@icao.int ;
	319.	Mr. Hiroyuki Takata	Regional Officer ATM APAC Regional Sub-Office International Civil Aviation Organization Asia and Pacific Office	htakata@icao.int ;
	320.	Dr. Manjit Singh	Acting Regional Director International Civil Aviation Organization Asia and Pacific Office	msingh@icao.int ;

ICAO Asia/Pacific Regional Cybersecurity webinar:
“Management Framework for CNS/ATM Systems”, 14 June 2021

(Video Teleconference, 14 June 2021)

	STATE/NAME		TITLE/ORGANIZATION	E-MAIL
	321.	Mr. Luo Yi	Regional Officer CNS International Civil Aviation Organization Asia and Pacific Office	yluo@icao.int ;
	322.	Mr. Remington Low	Regional Officer, Aviation Security and Facilitation International Civil Aviation Organization Asia and Pacific Office	rlow@icao.int ;
	323.	Ms. Soniya Nibhani	Regional Officer ANS (CNS) Implementation International Civil Aviation Organization Asia and Pacific Office	snibhani@icao.int ;
	324.	Ms. Pornrudee Ruthapichairak (Paula)	Business Development Officer International Civil Aviation Organization Asia and Pacific Office	pruthapichairak@icao.int ;
	325.	Mr. Philip Owara	IT Consultant International Civil Aviation Organization Asia and Pacific Office	powora@icao.int ;
	326.	Mr. How Sze Lung, Derek	Associate CNS Officer International Civil Aviation Organization Asia and Pacific Office	show@icao.int ;
	327.	Ms. Zhong Wenhan	Associate CNS Officer International Civil Aviation Organization Asia and Pacific Office	zmy07007@126.com ;
	328.	Ms. Bhabhinan Sirapongkosit	Programme Assistant CNS/MET/ENV International Civil Aviation Organization Asia and Pacific Office	bsirapongkosit@icao.int ;