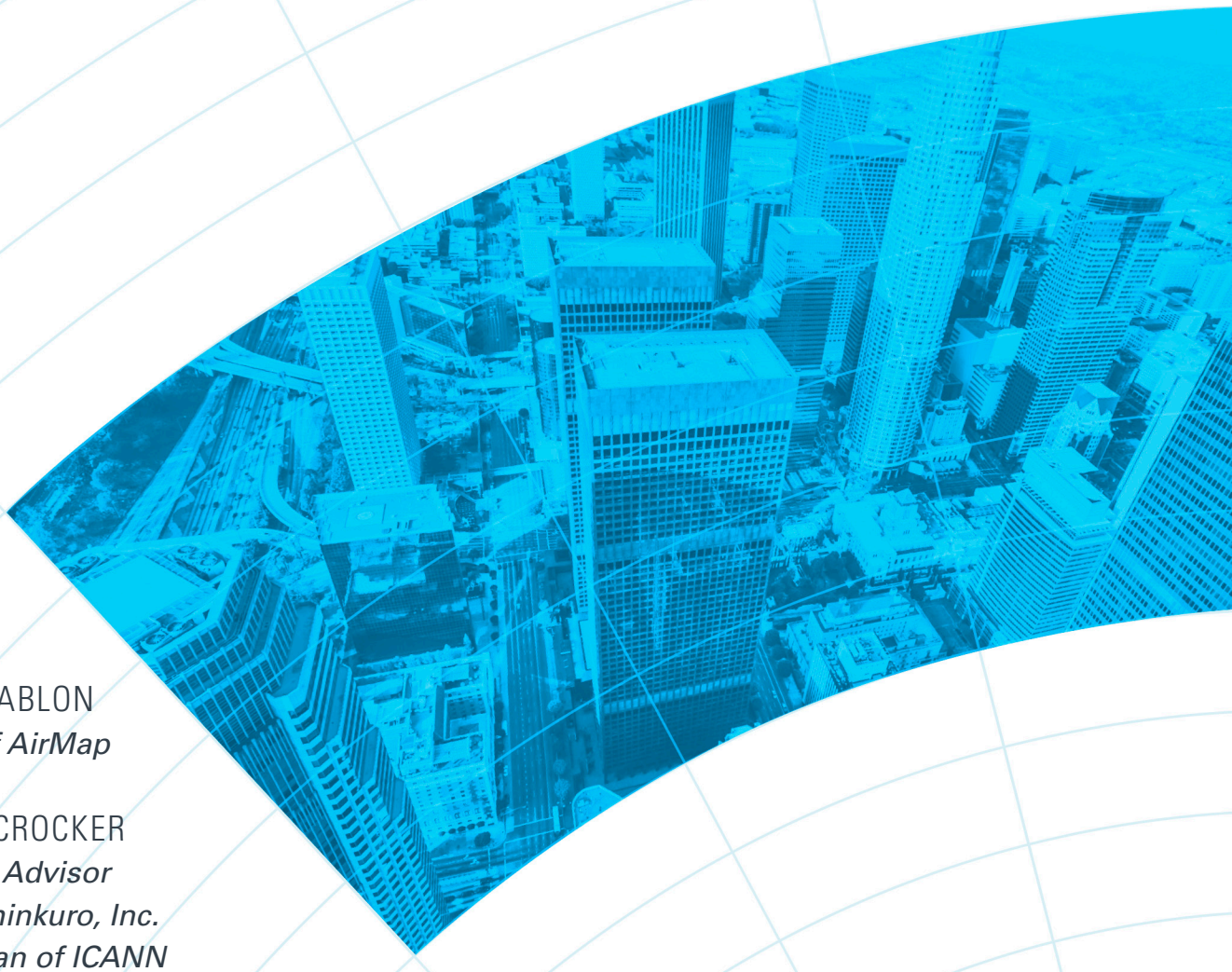
AIRMAP

Robust and Scalable UAS Registration:

KEY TECHNOLOGY ISSUES AND RECOMMENDATIONS



JARED ABLON
CISO of AirMap

STEVE CROCKER
AirMap Advisor
CEO, Shinkuro, Inc.
Chairman of ICANN

BENJAMIN D. MARCUS
CEO of AirMap

GREGORY S. MCNEAL
EVP of AirMap

Contents

Executive Summary

The growing Unmanned Aircraft Systems (UAS) ecosystem requires accountability of operators, availability of airspace, and security of communications, particularly a confidential, authenticated, and accessible registration system. The FAA's recent launch of a web-based registration service starts the UAS registration system in an excellent direction. Nevertheless, the scope and scale of the system's future capabilities remains a concern. The anticipated growth and diversity of UAS use suggests the need for a globally-integrated system more capable than today's.

A robust and scalable registration system considers the right technologies for its organization, registration information, queries, and security as the UAS ecosystem expands. This paper argues that careful selection of current Internet technologies and protocols can help enable the creation of a registration system that serves present needs but will also evolve as technology advances.

The paper makes eight core recommendations based on tried methods and available technologies:

1. ESTABLISH A THICK REGISTRY WITH EXTENSIBLE UAS OBJECT AND UAS ACTOR ENTRIES in order to manage the complexities and scale of a UAS registry/registrar system. Eventually there will be many front-end registrar services tailored to different UAS development and use scenarios but with all the details of registration residing in the registry. Initially, a registration entry should be defined as a simple, extensible object consisting of a UAS object and a UAS actor. This can be modeled on the International Registry of Mobile Assets.

2. PLAN FOR THE EVENTUAL SEPARATION OF THE REGISTRAR FROM THE REGISTRY though the two should initially be a combined entity, in order to easily support the initial millions of users. Once registrar and registry split, the service could handle billions of entries and would have better fault tolerance (e.g., if one registrar fails, another is available and can cache & queue information if the registry is down). An XML- and/or JSON-based system for passing registration information and queries makes it easy to add or remove fields in the future and helps keep the system extensible. Provide incentives for registrars to add and remove fields as the system evolves.

3. BEGIN WITH SIMPLE TLS QUERIES, BUT PLAN TO MIGRATE TO A SYSTEM THAT CAN MAKE USE OF RDAP helping the system scale to handle billions of queries. A basic Web registration and Web query system over TLS to a single, integrated database is simple to setup and can handle near term needs.

4. ARCHITECT THE SYSTEM TO ALLOW FOR CRYPTOGRAPHIC QUERIES IN THE FUTURE, similar to DANE, to help enable UAS to securely communicate with each other, other aircraft, and air traffic managers. Queries should initially allow for authorized users to look up basic information but as this system becomes the backbone for communication between the UAS, the number of queries will grow significantly. Using a DNS-like system will help allow for the evolution.

5. ESTABLISH A NEW PKI SYSTEM, for secure UAS communications. New UAS PKI Certificate Authorities should handle digital certification of public key ownership for all UAS. These keys will be used for both encryption and authentication of UAS data and communications. In the future, the registration system should help manage the public keys, similar to DANE. Each UAS should have its own private/public key pair in order to identify and distinguish it from others. UAS manufacturers will need to build the capability for securely storing a private key in the UAS. Best practices can be gleaned from smartphone manufacturers.

6. ADOPT DATA ENCRYPTION AND PII STANDARDS. Data should be sent via TLS. Data at rest should be encrypted with cryptographically strong algorithms such as AES. Certain Personally Identifiable Information (PII) about UAS operators should be kept private by allowing a registrar to provide their information as a proxy to the registry. Metadata should be protected and not freely given to anyone querying for data.

7. ESTABLISH PROCEDURES FOR AUTHENTICATION OF INFORMATION SOURCES, such as verification through a phone number with SMS verification or credit card information, which could be used in the near term. A longer term solution for identity verification could include submitting a drivers' license with additional credit information verification.

8. ESTABLISH PROCEDURES FOR AUTHENTICATION OF REGISTRY DATA, such as digital signatures for verification of authenticity against official, stored versions. Current web Certificate Authorities can be used for certification of public key ownership to support initial web queries. While this means that those making queries can be assured they are receiving an accurate copy of the registration information, there is a separate issue in ensuring that the registration information is, itself, accurate and complete. That requirement pertains to the quality control processes that are part of creating the registration.

Introduction

Airspace safety requires, at its foundation, reliable aircraft registration. On December 21, 2015, the United States Federal Aviation Administration (FAA) introduced a web-based registration service (see fig. 1) specifically for non-commercial small unmanned aircraft systems (sUAS). This represents a critical first step toward deployment of a scalable, secure registration system to ultimately support the need for identification and authentication of millions of unmanned aircraft systems (UAS) operating billions of flights. This paper identifies key challenges and needs of a UAS registration system and proposes recommendations.

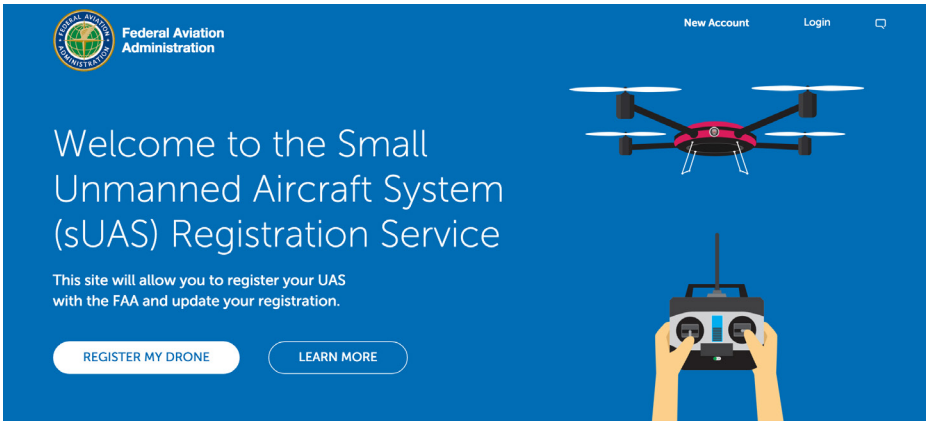


Figure 1

FAA sUAS Registration
http://registermyuas.faa.gov

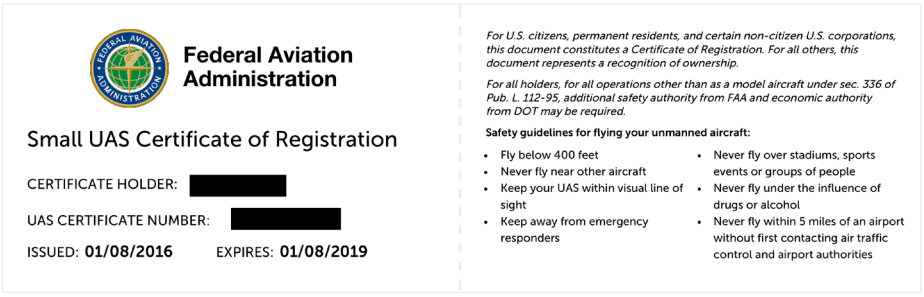


Figure 2

FAA sUAS Registration Certificate

The traditional aircraft registration system supports a few hundred thousand registrations and serves as a record of title to aircraft. The system functions well for its intended purpose and scale but is too slow to sufficiently serve UAS registrants. With the exception of being an aerial vehicle, a UAS has more in common with a smartphone than a 747. Yet the potential of UAS to deliver new, valuable services to hundreds of millions of people on a daily basis requires fundamental changes in registration methodology for such aircraft and the ability to make related queries. Experts predict near-term UAS registration requirements to eclipse traditional aircraft by ten to thirty times with long-term registration needs growing by orders of magnitude. On January 6, 2016, FAA Administrator Michael Huerta announced the sUAS registration system had logged 181,000 registrations (see fig. 2). With less than 30 days online, sUAS registration already accounts for over half the number of civil registered manned aircraft in the United States.

Soon the registration system for UAS will need to support more than the traditional functions of aircraft registration. The system will need to support queries by UAS, airports, aircraft, and private citizens. A properly architected registration system has the potential to act as the means to support routing communication and broadcast traffic between each of these entities. It could help facilitate a robust safety infrastructure as new features come online over time. For example, if an ADS-B-like system becomes the preferred method for communicating position information then adding authentication becomes crucial due to increased possibility of spoofing; the registry could manage PKI certificates for authentication.

While the relatively simple and centralized online system recently deployed by the FAA can handle the near-term needs of UAS operated within line-of-sight, the much-larger scale and autonomous characteristics of future UAS operations require evolution to a different type of model. In order to ensure seamless ease-of-use, availability to airspace, and security, the FAA needs to deploy a new model to take into account organization, registration, queries, and security.

I. GOALS AND CONCERNS OF A UAS REGISTRATION SYSTEM

System design necessarily requires navigating trade-offs. Evaluation should include clarity about the nature of the trade-offs and the rationale behind particular choices. System considerations should include: organization, registration information, queries, and security. These are delineated in the following sections.

A. ORGANIZATION - GOALS

How should the administration and operation of the registration system be organized? The simplest organizational model to understand is fully centralized and within a single entity. For basic efforts this typically works well. However, market and scaling pressures can dictate splitting up functions among different entities. For a registration system, an especially salient separation is between front-end (registrar) and back-end (registry) services:

- **Registrar:** The front-end services of interacting with registrants and others can be performed by one or more independent entities subject to common administrative and operational requirements.
- **Registry:** The back-end service of data storage and retrieval is typically performed by a single operator. When there are multiple registries, they must follow conventions for coordinating responsibilities.

The relationship between registrar and registry can vary:

- **Thick registry:** The registry holds all of the relevant registration information, including details about the registrant. Any registrar might be able to process the next transaction for the entry. The capabilities of the registrar are therefore kept basic.
- **Thin registry:** The registrar retains portions of the basic registration, such as the registrant's name or contact information. The role of the registry is reduced.

"While the relatively simple and centralized online system recently deployed by the FAA can handle the near-term needs of UAS operated within line-of-sight, the much-larger scale and autonomous characteristics of future UAS operations require evolution to a different type of model."

B. REGISTRATION INFORMATION - GOALS

The core activity of creating registrations needs to be based on a number of essential design attributes, specifically:

Identification: The activity of a UAS is the result of multiple actors each of which must be uniquely identified and correlated with a specific device -- the Manufacturer (including hobbyists and amateur makers); the Owner (including fleet owners); and the Operator (with the possibility of autonomous operations and single operator multiple aircraft).

Scalability: For the near term, the system must support low millions of registrations. For the longer term, the target should permit capabilities into the low billions.

Extensibility: An initial system will be useful with minimal capabilities; a basic set of information and functions will suffice. Relative simplicity will make the system easier to develop, deploy, and use. The design also needs to be flexible enough to support the addition of new types of information and use cases. The only way to evaluate a design for such extensibility is to conduct sample scenarios for introducing changes that are deemed realistic.

C. QUERIES - GOALS

The second half of a registration system is making registration information available and accessible. The functional and performance requirements affect design choices and are composed of use, scalability, population, and type.

Use: What are the required uses of the registration? Desired uses? Who is authorized for such uses? For example,

should the registration database be used to authenticate the operator that creates a flight plan trajectory? Should the database be accessible by members of the public who wish to identify the operator of a specific UAS seen operating near them? Should law enforcement be able to use the database to identify bad actors?

Scalability: Just as scaling requirements for registrations affect design, so do the number and rate of queries. A system needed only for exceptional queries, in special circumstances and only by a limited number of authorized agencies, permits a very different design from one that must support widespread and frequent use by the general public. What are the near-term and longer-term targets for number and rate of queries and for query response latency?

Population: A system that may be used only by a small number of authorized participants (for example the FBI's criminal database) can be constructed in relative isolation. One that must be accessible to a much broader audience (for example DNS) requires essentially public access. The design choices for a smaller, private service are substantially easier than for a public one.

Type: Simple queries ask for some or all of the static information associated with a registration (for example the manufacturer of a UAS). Queries for dynamic information pertain to current or on-going activities related to the registration (for example current location of the UAS or the current operator). What are the near-term and longer-term requirements for types of queries? Should queries for 'dynamic' information be treated as part of the registration system or as outside of it, and specifically as a 'customer' of the registration system?

D. SECURITY[1] - GOALS

A number of specific concerns need to be addressed under the general rubric of "security". Most importantly, the information must otherwise be kept private (confidentiality); it must be verified to be correct and unable to be altered incorrectly (integrity); and the information must be available when needed (availability).

Confidentiality: There must be assurances that data can only be accessed by authorized parties. One method of protecting against unauthorized disclosure is through data encryption, both in transit and at rest. Privacy is also an important aspect of such a registration system.

- **Data encryption in transit:** Protection as part of the data transfer service.
- **Data encryption at rest:** Protection of stored data when not in use.
- **Privacy of content:** Only authorized recipients should have access to the information they are allowed to access. If all information is fully public, privacy is a relatively minor issue. As soon as some or all of the information is deemed private and is subject to rules for disclosure, privacy becomes extremely challenging, particularly when the system has a broad base of users.
- **Privacy of context (e.g., metadata):** Specific attention needs to be given to the handling of information that is associated with the basic registration. This includes static attributes of the registration that are not part of the core information, such as registration date versus name of registrant. It also concerns details about activity on the registration, such as who makes queries and when. Even without access to the content of the registration, a bad actor can take advantage of knowledge about query activity.

Integrity: There must be assurances that the initial information transmitted is the same as the information recorded, registered, and maintained, unless modified by an authorized party.

- **Authentication of information source:** Certifying the identity of an agent providing or modifying the information and possibly certifying the identity of the recipient serve as the underpinning of accountability of accurate information.

Availability: The system must be accessible by interested and authorized parties when needed. This includes both for registration, and possibly more importantly, for queries.

II. LESSONS FROM THE INTERNET

The Internet provides many examples of database and security technology failures and successes. Common confusion about original goals for some of the technologies, as well as limitations of their actual uses, only confuses matters. For any proposed use of an Internet-related technology, discussion needs to ensure clear and accurate understanding of the actual experiences with it.

By way of example, consider X.509 certificates and the general Public Key Infrastructure (PKI) intended to validate the association between a specific cryptographic key and a specific Internet domain name or email address, now in widespread use but with ongoing administration problems.

[1] *Security best practices for the system are assumed. Only a few important external design decisions are discussed throughout the paper.*

In general, PKI works well within smaller communities that have well-established trust relationships or large authoritarian communities (e.g., the U.S. Department of Defense) but poorly for larger-scale, complex uses. In fully public venues, PKI is widely used to identify web and email servers. However, problems with broad-based administration and use of PKI have prompted many of the organizations running these servers to self-certify. That is, they act as their own root to the PKI hierarchy. In effect, every web browser in the world has to make a trust decision about potentially many thousands of independent PKI roots. In addition, the efficacy of particular algorithms used in PKI may be a problem (RSA, Elliptic Curve, SHA1, etc), especially with ongoing evolutions in quantum computing.

In terms of global database services, the World Wide Web might be counted as a large, complex, and distributed example. However, the interconnection between independent sites is extremely loose and administration is inconsistent. A more useful example of success is the Domain Name System (DNS), which maps web and email addresses to underlying network (IP) addresses as well as providing other information such as cryptographic signature details associated with a domain name. Arguably, it is the only large-scale, global database in operation over the Internet subject to integrated administration and operations policies. It has demonstrated remarkable scaling and data storage flexibility. However, it also requires all information to be fully public. There are current efforts to make query activities more private but this is a nascent specification task with no implementation, deployment, or use experience. In addition, DNS has its share of security issues due to lack of authentication and encryption. There are slow-to-be-adopted efforts to remedy this.

Nevertheless, Internet technologies can provide a roadmap to address concerns surrounding a viable UAS registrations system. Below are considered only those publicly available standard technologies with an established track record.

A. ORGANIZATION - LESSONS

Digitally-based services introduce challenges in authentication and privacy, especially when the perceived value of a registration is high. For example, what is the value of being able to attribute the registration of a rogue UAS to a different party?

As long as the registration system is operated by a single organization and has a narrow scope of functionality requirements, a simple, online web interface and almost any back-end database will suffice for registrations in the millions. Similarly, a modest web-based query interface will suffice. To the extent that such a system needs cloud-like distributed computing and storage, this can be hidden behind the online interfaces. Such operations are common in today's Internet.

As the registration system grows in scale and functional needs so too does the potential need to support many independent registrars and even multiple, independent registries. That is, it might prove helpful to divide the space of registration values for independent administration. DNS is the only Internet example of an operation functioning at a scale similar to the future UAS ecosystem. However, a UAS registration system is likely to need much more centralized control over rules of operation and content for entries. In order to make it easy for any UAS owner/operator to register, it will be particularly helpful to specify a standardized Application Programming Interface (API) giving write access to the registration system. This will allow development of a drone manufacturer's app or other apps popular amongst UAS operators making it easier for anyone to register and thereby significantly increase compliance with the registration mandate. Finally, provide incentives for app developers to stay up-to-date with the latest API as the system evolves.

One established Internet registration technology related to allowing write access:

Extensible Provisioning Protocol (EPP) [RFC 5730]

This is used by DNS registrars to create and modify domain name entries with the relevant registry. It is in extensive use.

B. REGISTRATION INFORMATION - LESSONS

Several Internet technologies have facilitated the evolution of information transmission, formatting, and access including:

Identification: The foundation of any registration is the assigned identifier. Choices such as a simple, serially-assigned number, a random string, or a human-friendly text string depend on expected use and the effort needed to make the registration. It is tempting to suggest a scheme to satisfy multiple goals but this can introduce problematic complexities. In particular, a scheme that effectively registers two or more values – such as a serial number combined with a human-friendly string – invites synchronization challenges.

- **Simple Textual Encoding:** Concern for efficient storage of data often drives designers towards complex

and obscure encoding conventions. This is rarely necessary today. It is usually far better to start with a simple format that is easily understood by the humans who must work with the information. In some specialized scenarios, more storage-efficient encoding may be needed for which simple mapping can be specifically developed.

- **Separating Object from Transfer Mechanism:** When properly designed, data can be specified as an object capable of carriage through different mechanisms. Objects such as an email message or a Web page can be transported through a variety of mechanisms resulting in a useful flexibility helpful for new systems likely to undergo unanticipated changes. An initial design requirement should be to anticipate this separation even though initial use might only target fully integrated operation by a single provider or with a single data encoding and exchange pair. The separation facilitates migration to new forms of encoding or transfer.

Stability: For critical infrastructure, the registration system must prevent and/or be resilient to failures, including organizational failures. How will the system handle failure of a registrar? What will prevent failure of a registry?

- **Separating Registrar from Registry:** As discussed earlier, the front-end and back-end registration activities typically can and should be separated for large-scale operation. For DNS, this separation works successfully at a global scale.

Extensibility: When choosing a scheme for registration values, it is tempting to define fields that enforce interesting semantics onto some parts of the value. For example, a registration value might indicate where the registration was performed or when or the type of specific registration. When the uses of the values are extremely well understood and future flexibility is known to be limited this can work well. Similarly, some aspects of registration operation or use might dictate creation of such semantics. However, in general, basic semantic-neutral registration schemes work better in the long term because they leave the most flexibility for later development.

C. QUERIES - LESSONS

The simplest early planning assumption about the level of activity for the registration system is for bursts of tens or hundreds of thousands of registrations (correlated with holiday gift-giving, for example) combined with occasional queries in the range of hundreds or perhaps thousands per day (for law enforcement investigations, for example). Any online system can handle this load easily. A simple, web-based interface will suffice for accessing it.

As the number and sophistication of UAS operations grow, APIs will be necessary for better integration to apps and external services.

There are many models available with different needs for Use, Scalability, Population and Type. A brief summary of established, Internet-query technologies follows as a way of demonstrating different models for a UAS registration system.

1. WHOIS (RFC 3912) WHOIS is a very basic protocol for querying a public registration database. It uses a simple string to query, obtaining a free-form block of text as the response. Response information includes details about the owners of Domain names registered in the DNS. Many users of WHOIS have imposed conventions in the format of the response, but these are applied inconsistently. More significantly, each WHOIS databases independent of the others; that is, its base for queries is only a subset of the total DNS. The linkage between WHOIS databases is loose or absent.

2. Registration Data Access Protocol (RDAP) [RFC 7482] Over the years, a number of efforts have been made to replace WHOIS. The latest is the Registration Data Access Protocol (RDAP). RDAP provides structured queries and responses, permits authentication and access control, and can support differential responses based on local policies. There is limited field experience. While it has significant deployment among providers of information, there is limited adoption among data consumers.

3. Domain Name System (DNS) [RFC 1035] The DNS (see fig. 3) is a global, distributed, integrated mapping service using a fixed domain name string to retrieve associated information such as an IP address or a cryptographic key. The service supports only public queries, although private versions of the DNS are operated by various organizations (for example communications carriers use DNS to resolve Internet telephone calls).

DNS data is historically stable with changes to specific entries tending to take place across months or years rather than minutes or seconds. However, there are DNS enhancements to support much more dynamic updating activities.

The benefit of using DNS is its extensive operational experience including unique demonstration of massive scaling across very large numbers of independent administrations. The detriment of using the DNS is its simple data model and restricted query functionality. In particular, it is intentionally only a simple mapping service rather than a full database query capability with generalized searching capabilities.

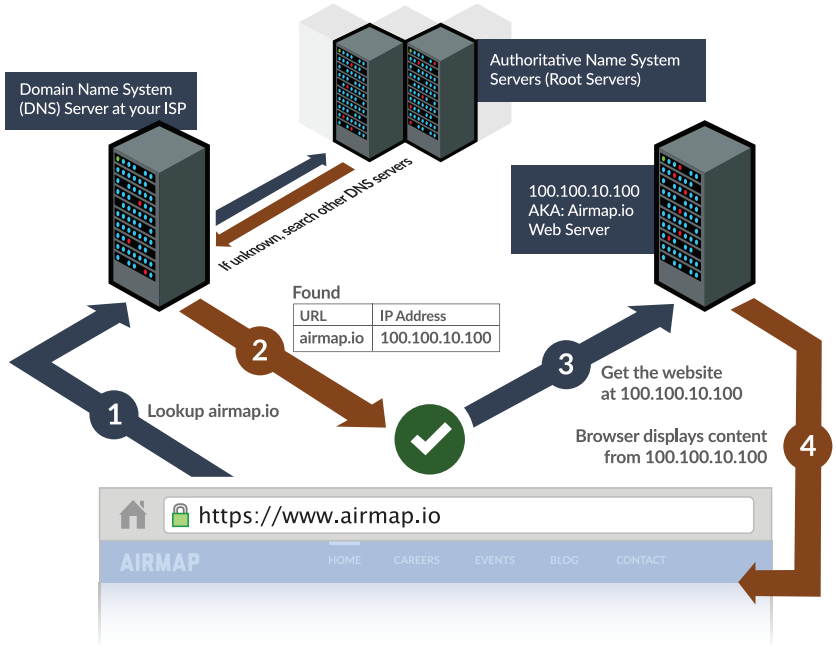


Figure 3

How DNS Works

4. Lightweight Directory Access Protocol (LDAP) (RFC 4511) Lightweight Directory Access Protocol (LDAP) is used within enterprise networks to connect, search, and modify Internet directories. LDAP has not seen successful use as an integrated service across multiple independent administrations.

D. SECURITY - LESSONS

The Internet technologies that relate to security overlap between Confidentiality, Integrity, and Availability (CIA). The specific Internet technologies considered are all discussed following the discussion of CIA.

Confidentiality:

- **Data encryption in transit:** One common way for encryption over the Internet is passing a session cryptographic key via asymmetric cryptography (i.e. public/private key algorithms). The session key is then used to encrypt and decrypt the data in transit.
- **Data encryption at rest:** There are many ways to encrypt data at rest and still allow access when needed. Strong algorithms should be used such as the Advanced Encryption Standard (AES).
- **Privacy of content and context/metadata:** Methods of protecting information against unauthorized disclosure work well over the Internet only within small or tightly-controlled environments. Potential policy-drivers requiring privacy might include protection of individual freedom of speech or protection of intellectual property or trade secrets of businesses using UAS.

Integrity:

- **Authentication of information source:** The Internet uses many different techniques for verifying that a participant is who they claim to be. Email addresses, SMS phone number verification and credit card numbers enable popular, basic validation at Internet scale. Some more extensive verification over the Internet is in the form of ID verification with additional credit report questions. However stronger, cryptographic-based forms of authentication have generally proved more difficult at Internet scale. Where an identity is subject to serious validation, so that authorizations and accountabilities related to the person or organizations having the identity are substantive, digital authentication has proved viable only in very constrained environments with prior arrangement and usually within a single administration or a single confederation.

Availability: The Internet was built on the model of having a distributed infrastructure with no single point of failure. This distributed concept was extended with DNS and allows for a highly available system globally. Similar concepts can help provide a highly robust UAS registration infrastructure.

The following brief summary considers those established Internet security-related technologies capable of being re-purposed for UAS registration system use:

1. X.509 Public Key Infrastructure (PKI) [RFC 5280]
PKI (see fig. 4) is the preeminent mechanism on the Internet for associating an identifier with a public key. The

PKI model is based upon a hierarchy of trust, where the Internet's set of "root" registries is unfortunately large. The root Certificate Authority validates subordinate authorities, who then certify authorities below them, and so on. As previously mentioned, its deployment and administration have proved challenging. As with many other Internet technologies, the most substantive uses of PKI are within constrained administrative and operational environments, such as an industry association. PKI can help with Confidentiality (data encryption) and integrity (source authentication via digital signatures).

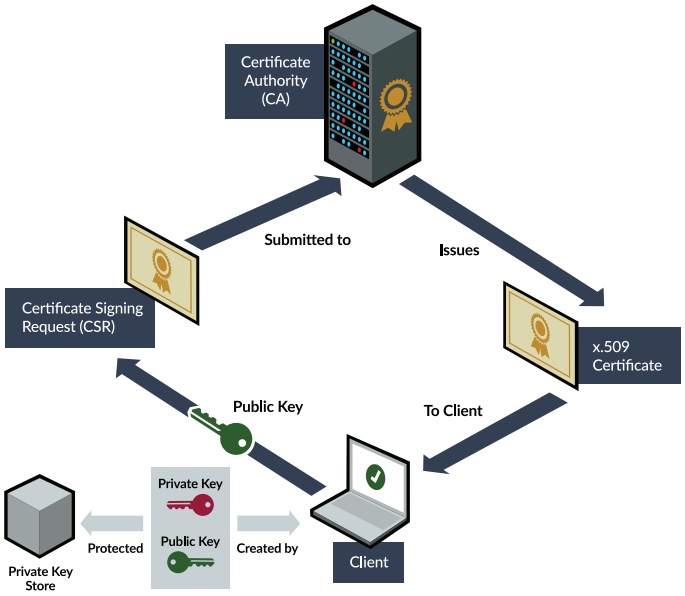


Figure 4

How PKI Works

2. Domain Name Security (DNSSEC) [RFC 4033]
DNSSEC creates a limited PKI, solely for validating the contents of the DNS naming hierarchy (integrity). Its adoption is increasing but still remains limited.

3. DNS-Based Authentication of Named Entities (DANE) [RFC 6698]
In response to the continued problems with use of PKI for Internet functions such as validation of keys used for encryption in Internet services, a narrow effort was started to create a simplified trust hierarchy tied directly to the DNS. DANE currently has enthusiastic support but, again, very limited field experience especially among client software.

4. Transport Layer Security (TLS) [RFC 5246]
TLS provides channel encryption and is very widely used for Internet services. It is capable of validating both the client and the server in the connection, however only the latter is widely performed. Unfortunately, the use of self-signed PKI certificates with TLS means that the client cannot always adequately validate the server. This leaves the exchange open to spoofing, in particular Man-In-The-Middle (MITM) attacks. DANE is an effort to improve upon this situation.

5. OAuth [RFC 6749]
This mechanism permits a service to obtain user authentication through a separate identity provider. Notably, this permits the service to validate a user without seeing the user's password, but only if the current service trusts validations made by the identify provider acting as the user's "home." OAuth has recently gained significant use.

6. OpenPGP [RFC 4480] and S/MIME [RFC 3851]
These provide object encryption and have many software implementations. S/MIME uses the PKI, while OpenPGP innovated an ad hoc Web of Trustmodel. Both technologies have been in some use for nearly 20 years but neither has gained widespread use in open, inter-organization settings.

III. RECOMMENDATIONS

Given the urgent need for UAS registration, the web-based system recently introduced by the FAA is an excellent starting place for global adoption. The state of existing, Internet-scale technologies makes it possible to pursue this modest initial capability in a manner allowing for substantial future evolution. An underlying concern is the scope and scale of each aspect of the registration system. The expected scale and diversity of UAS use suggests the need for a globally-integrated capability.

Below are proposed recommendations for developing a UAS registration system with particular consideration to organization, registration, queries, and security (see fig. 5).

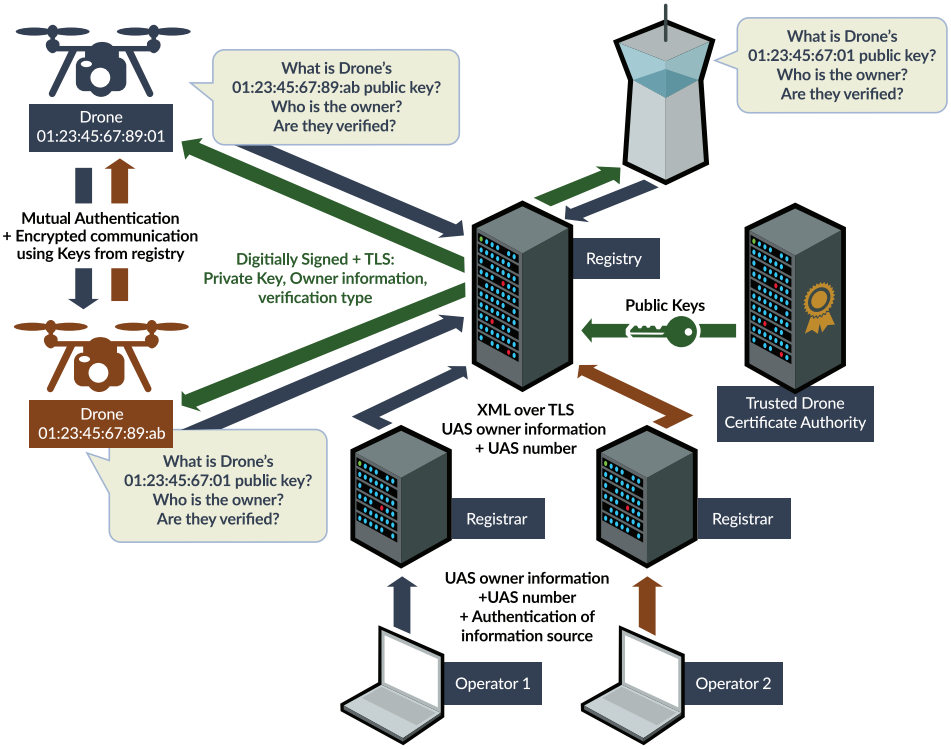


Figure 5

Proposed Registration System

A. ORGANIZATION - RECOMMENDATIONS

Establish a thick registry with extensible UAS object and UAS actor entries in order to manage the complexities and scale of a UAS registry/registrar system. Eventually there will be many front-end registrar services tailored to different UAS development and use scenarios but with all the details of registration residing in the registry. Initially, a registration entry should be defined as a simple, extensible object consisting of a UAS object and a UAS actor. This can be modeled on the International Registry of Mobile Assets.

Given the need for tight quality control on registration information and for operational assurances about availability of the information, it is possible that only a single registry is appropriate. The registry could be managed by one entity or an alliance that includes various stakeholders. In any event, there should be a clear model for oversight and governance of the registration system, in order to provide assurances about registrar operators, registry operators and registry entries.

Interaction between registrars and the registry should to be standardized. EPP could be useful for this function and could help extend the solution as required.

B. REGISTRATION INFORMATION, RECOMMENDATIONS

A registration entry should be defined as a simple, extensible object. An example of such an object should consist of a UAS object and an Actor object:

- **UAS**: Basic registration information for a UAS, for example manufacturer, model, serial number, and owner.
- **Actor**: Basic registration information for a person or organization and their UAS role.

This is quite similar to how the International Registry of Mobile Assets works. The International Registry was established under the legal framework of the Cape Town Convention and Aircraft Protocol, which is an international agreement between participating nations to help optimize the registration, sale, and financing of aircraft around the world.

Identification: As a simple starting point, a single identifier value can be used to indicate a UAS owner and a UAS. Initially, an identifier value similar to an Ethernet MAC address could be used to simply and easily identify the manufacturer, model, and individual UAS. Additionally, having a unique value that identifies the UAS owner could

help pair owners with their particular UAS and allow for instances of UAS ownership transfers. Initially, the owner will be responsible for the UAS, however, in the future a UAS operator may be responsible party which could give rise to a licensing system.

These identifier values should have a structured format to support a distributed administrative assignment model, such as is currently done for Domain Names, IP Addresses, and Ethernet MAC addresses.

Scalability: Plan for the eventual separation of the registrar from the registry though the two should initially be a combined entity, in order to easily support the initial millions of users. Once registrar and registry split, the service could handle billions of entries and would have better fault tolerance (e.g., if one registrar fails, another is available and can cache & queue information if the registry is down).

Extensibility: An XML- and/or JSON-based system for passing registration information and queries makes it easy to add or remove fields in the future and helps keep the system extensible. Provide incentives for registrars to add and remove fields as the system evolves, otherwise they may lag behind as the system changes.

C. QUERIES - RECOMMENDATIONS

Begin with simple TLS queries but plan to migrate to a system that can make use of RDAP helping the system scale to handle billions of queries. A basic Web registration and Web query system over TLS to a single, integrated database is simple to setup and can handle near term needs.

Use: Queries should initially allow for authorized users to look up basic information but as this system becomes the backbone for communication between the UAS, the number of queries will grow significantly. Using a DNS-like system will help allow for the evolution. In the future, the system could be used to look up cryptographic key information, similar to DANE, so UAS can securely communicate with each other, other aircraft, and air traffic managers.

Scalability: In the near term, with existing use cases and the number of operable UAS, the number of queries will likely be low. However, as this system becomes the backbone for communication among UAS, the number of queries could grow significantly. Using a DNS-like system could help allow for the growth that is expected.

Population: It is recommended that the system and information within the system be publicly available and editable by authorized parties. However, if a registrant would like to keep certain personal information private, and policy allows, individuals should be able to opt for privacy during registration with the registrar in a way similar to how people can opt for registering domain names in a private manner. In order to allow for flexibility, there should be the potential for some private information to be accessible to certain entities, such as governments or air traffic managers. This private information could be accessible after authentication to the registration system.

Type: The types of queries will be for static information only. Some information could change occasionally (for example, the UAS owner), but information such as the location of a particular UAS would be a part of a separate system. That said, the registration system could help support the dynamic information queries. For example, public keys can be queried in the registration system and they can be used for secure communication and/or digital signing of critical information.

"The state of existing, Internet-scale technologies makes it possible to pursue this modest initial capability in a manner allowing for substantial future evolution."

D. SECURITY - RECOMMENDATIONS

In order for the registration system to support robust UAS communications, new UAS PKI Certificate Authorities should handle digital certification of public key ownership for all UAS. These keys will be used for both encryption and authentication of UAS data and communications. In the future, the registration system should help manage the public keys, similar to DANE. Each UAS should have its own private/public key pair in order to identify and distinguish it from others. UAS manufacturers will need to build the capability for securely storing a private key in the UAS. Best practices can be gleaned from smartphone manufacturers.

Confidentiality: Proposed recommendations for protecting information for both data encryption and privacy are outlined below.

- **Data encryption:** Data should be sent via TLS and data at rest should be encrypted with cryptographically strong algorithms such as AES.
- **Privacy of content and context/metadata:** Certain Personally Identifiable Information (PII) about UAS operators should be kept private by allowing a registrar to provide their information as a proxy to the registry. In addition, metadata should be protected and not freely given to anyone that queries for the data.

Integrity:

- **Authentication of information source:** In order to handle near term needs, a phone number with SMS verification or a credit card should be used to verify identity. A longer term solution for identify verification could include drivers' license submission with additional credit information verification. It is important to denote the method of authentication in order to distinguish between different trust levels as the system evolves.
- **Authentication of information from the registry:** Registration data should be digitally signed so that its authenticity can be verified against the official, stored version. Since web queries are going to be used initially, current web certificate authorities can be used for the certification of public key ownership. While this means that those making queries can be assured they are receiving an accurate copy of the registration information, there is a separate issue in ensuring that the registration information is, itself, accurate and complete. That requirement pertains to the quality control processes that are part of creating the registration.

Availability: With the proposed initial web-based system, availability could be an issue. However, the current registration system does not seem integral to the functioning of the initial UAS ecosystem. As autonomy comes about and the ecosystem evolves, the registry should evolve towards ensuring high availability. In the future, using the proposed distributed registrar/registry system should allow for a more robust system not reliant on a single point of failure.

IV. CONCLUSION

Accountability of UAS operators, availability of airspace, and security of communications are critical for the growing UAS ecosystem. Ensuring this requires a registration system that considers solutions for organization, registration information, queries, and security. It is imperative to select the right technologies to build a robust system that scales with the UAS ecosystem. Careful selection of current Internet technologies and protocols can help enable the creation of such a registration system for today and can shift with an industry having the potential to reshape our tomorrow.

About AirMap

AirMap is the world's leading provider of aeronautical data and services to unmanned aircraft. AirMap's real-time services are available to manufacturers through an API and through an SDK for application developers. AirMap is heavily focused on aviation safety and innovation and recently announced the integration of their aeronautical data into leading consumer and light commercial unmanned aircraft, including those manufactured by companies like DJI and 3DRobotics. AirMap also provides aeronautical data to over 200 software developers who are making apps for unmanned aircraft. Those developers will be able to create apps for unmanned aircraft operators seeking to file flight notifications as part of the AirMap D-NAS system.

The founders of AirMap are among the world's foremost experts on unmanned aircraft technology, aviation, and policy. The company is dedicated to ensuring the safe integration of unmanned aircraft into everyday life and is committed to providing accurate airspace information and safety critical communication links and services that foster innovation while protecting public safety. AirMap is a member of the Association of Unmanned Vehicle Systems International (AUVSI), a sponsor of the Know Before You Fly Campaign, a participant in NASA's Unmanned Traffic Management (UTM) program, and served on the FAA's UAS Registration Task Force.

Author Bios

JARED ABLON

CISO of AirMap

Jared Ablon is AirMap's Chief Information Security Officer (CISO). Ablon has more than 12 years of experience in both offensive and defensive security. Most recently, he worked at MITRE Corporation, where he led efforts to ensure security of next generation GPS navigation systems and other communications technologies for multiple U.S. Air Force programs against some of the most sophisticated attacks. Ablon founded Passrock, which developed a commercial fraud prevention solution for businesses to mitigate the risk of stolen users accounts. He started his career at the U.S. Department of Defense where he led large teams of security experts and tackled nearly intractable problems by developing cutting-edge cryptanalysis, network exploitation, and vulnerability analysis security technologies. Ablon earned a B.A. in Applied Mathematics from the University of California at Berkeley, an M.S. in Applied and Computational Mathematics from Johns Hopkins University, an MBA from the University of Maryland, and holds a Certified Information Systems Security Professional(CISSP) credential from the International Information System Security Certification Consortium (ISC)[2].

STEVE CROCKER

AirMap Adivisor, CEO of Shinkuro, Inc. and Chairman of ICANN

Dr. Crocker is CEO of Shinkuro, Inc., a small company based in Bethesda, MD focused on advanced security and collaboration technology technology, and is Chairman of the Board of the Internet Corporation for Assigned Names and Numbers. It promotes competition and develops policy on the Internet's unique identifiers. Through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

Dr. Crocker has been involved in the Internet since its inception. In the late 1960s and early 1970s, while he was a graduate student at UCLA, he was part of the team that developed the protocols for the Arpanet and laid the foundation for today's Internet. He organized the Network Working Group, which was the forerunner of the modern Internet Engineering Task Force and initiated the Request for Comment (RFC) series of notes through which protocol designs are documented and shared. For this work, Dr. Crocker was awarded the 2002 IEEE Internet Award. Dr. Crocker also holds an honorary doctorate in mathematics from the University of San Martin de Porres in Lima, Perú. In 2012, Dr. Crocker was inducted into the Internet Hall of Fame - Pioneer

Circle, recognizing him as an individual who was instrumental in the early design and development of the Internet.

Dr. Crocker's experience includes research management at DARPA, USC/ISI and The Aerospace Corporation, vice president of Trusted Information Systems, and co-founder of CyberCash, Inc. and Longitude Systems, Inc. His prior public service includes serving as the first area director for security in the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the IETF Administrative Support Activity Oversight Committee (IAOC), service on the Board of the Internet Society and the Board of The Studio Theatre in Washington, DC.

Dr. Crocker earned his B.A. in mathematics and Ph.D. in computer science at UCLA, and he studied artificial intelligence at MIT.

BEN MARCUS

CEO of AirMap

Ben Marcus is CEO and co-founder of AirMap. Marcus is an FAA-certified Airline Transport Pilot and Flight Instructor with over 4,000 hours of flight experience in more than 100 aircraft types. He has been passionate about aviation his entire life, starting with remote-control airplanes. Marcus grew up in the shadows of the Santa Monica airport, took his first flying lesson at age 10, became a licensed pilot at age 17, and attended Purdue University's School of Aeronautics. Marcus strongly believes UAS will have an immense and positive influence on our lives providing valuable resources for public safety professionals, agricultural applications, package delivery, cinematography, and for many other inventive purposes. Prior to AirMap, Marcus co-founded jetAVIVA, the largest aircraft sales company in the world that centers on light jets. Marcus serves as vice-chairman of Angel Flight West, where he has volunteered for over twenty years.

GREG MCNEAL

EVP of AirMap

Gregory S. McNeal, JD/PhD, is a co-founder of AirMap and a professor of law and public policy at Pepperdine University. Dr. McNeal, has on multiple occasions testified before Congress and state legislatures about the legal and policy issues associated with drones and has aided state legislators, cities, municipalities, and executive branch officials in drafting legislation and ordinances related to drones. He has met with and provided input to the White House's Office of Management and Budget about the FAA's pending drone regulations. He also was appointed by the Secretary of Transportation to serve on the Unmanned Aircraft System Registration Task Force.

Dr. McNeal serves as a voting member of the ASTM technical committee creating scientific standards to govern unmanned aircraft and their operation, he is also a member of the Association of Unmanned Vehicle Systems International technical advisory and advocacy committees, serves as a board member of the UAVUS and sits on the advisory council for the Humanitarian UAV Network. He has advised unmanned aircraft start-ups, sensor manufacturers, law enforcement, consulting firms, insurance companies, and Fortune 500 companies about the legal and regulatory issues and benefits associated with UAS technology.