COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 4
Identity Management of Non-Person Entities

Table of Contents

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	10/24/2017	Initial Draft of Document

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from the Identity Management Standards Advisory Council (IMSAC).

- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.

3 Purpose and Scope

Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to establish minimum specifications for identity management of Non-Person Entities, so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. The guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

4 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for Identity Management of Non-Person Entities. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

Governing Statutes:

Secretary of Technology
§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council
§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act
Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

5 Definitions

The terms used in this document comply with definitions in the Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the Commonwealth of Virginia's ITRM Glossary (ITRM Glossary). [1]

The definitions may be accessed at:
http://vita.virginia.gov/default.aspx?id=6442475952

[1] NIST SP 800-63-3 may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3 . At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.
§ 59.1-550, *Code of Virginia*, may be accessed at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/
The Commonwealth's ITRM Glossary may be accessed at
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf

6 Background

In 2015, Virginia's General Assembly passed the Electronic Identity Management Act (Chapter 50 of Title 59.1, *Code of Virginia*) to address demand in the state's digital economy for secure, privacy enhancing Electronic Authentication and identity management. Growing numbers of "communities of interest" have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in §59.1-550.

Purpose Statement

This guidance document, as defined in § 2.2-4001, was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, the document establishes minimum specifications for identity management of Non-Person Entities (NPEs) in a Digital Identity System. The minimum specifications also outline a data model for interoperability and discovery of identity information on NPEs.

The document assumes that specific business, legal, and technical requirements for NPEs will be established in the Identity Trust Framework for each distinct Digital Identity System, and that these requirements will be designed based on the Electronic Authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL) requirements for the system. The document limits its focus to identity management for NPEs. Minimum specifications for other components of a Digital Identity System have been defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

7 Minimum Specifications

Identity management (IdM) of Non-Person Entities (NPEs) has become a critical issue with the growth in number and level of interconnectedness of "smart" devices, particularly as these devices increasingly become targets of malware and cyber attacks. Despite a substantial focus worldwide on IdM of person entities, the parallel effort on IdM of NPEs has not achieved a similar level of maturity.

The National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-63-3, and through the National Program Office of the National Strategy for Trusted Identities in Cyberspace (NSTIC), has established processes, protocols, and related guidance for IdM on persons but has not offered the same level of treatment for NPEs. Federal and State Identity Credential Access Management (FICAM/SICAM) Guidelines reference NPEs but do not define specific protocols for NPE management.

In recent years, international organizations have made substantial contributions to the knowledge-base relating to IdM of NPEs. Much of this effort stems from analysis on the "Internet of Things" (IoT), defined by the International Telecommunication Union (ITU) as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[2]

The European Commission IoT Expert Group's Subgroup on Identification, in its current-state analysis of the IoT, noted the following issues associated with IdM of NPEs:

- Object Identifiers and Protocols: The question of whether to adopt a global, standardized scheme of unique identifiers for NPEs or continue to maintain an array of distinct identity spaces for NPEs with fluctuating degrees of interoperability.
- Identifiers vs. Network Addresses: The importance of distinguishing between an NPE's identifier, which establishes a unique handle for the entity, and its network address, which may change based on the NPE's physical location.
- Resolution and Discovery Functions: The need to build upon existing knowledge and experience with identification, naming, and addressing systems to resolve disparate identifiers for an NPE and enable discovery across disparate Digital Identity Systems.[3]

The European Commission, and other groups such as the Cloud Security Alliance, Kantara Initiative, and Internet Society have published guidance on how to address these and related issues for IdM of NPEs.[4] Also, the ITU has released recommendations to promote interoperability, resolution, and discovery of identity information on NPEs.[5]

---

[2] International Telecommunication Union. 2012. *Recommendation Y.2060: Overview of the Internet of Things*. https://www.itu.int/rec/T-REC-Y.2060-201206-I

[3] European Commission. 2012. IoT Factsheet – Identification. Report from the Internet of Things Expert Group (IoT-EG), Subgroup on Identification. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12

[4] Cloud Security Alliance. 2016. *Identity and Access Management for the Internet of Things – Summary Guidance*. https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

The minimum specifications defined in this document leverage the guidance and recommendations issued by these international organizations. First, the minimum specifications set general guidelines for IdM of NPEs based on the guidance from the Cloud Security Alliance and Kantara Initiative. Second, the minimum specifications outline a standard data model for NPE identity information conformant with ITU recommendations.[6] Third, the minimum specifications present a comprehensive use case illustrating the complexity of issues associated with IdM of NPEs and strategies for addressing these issues through a standards-based reference architecture and communications protocols, such as those established by the European Commission and Internet Society.

General Guidelines

The following general guidelines have been adapted from the CSA's *Identity and Access Management for the Internet of Things – Summary Guidance.*

1. Integrate IdM-NPE implementation into existing IdM and IT governance frameworks. Considerations should include the following steps:
    a. Define a common namespace for NPEs.
    b. Establish an extensible identity lifecycle that can be applied to NPEs, designed based on the lifetime of the NPE and required identifier.
    c. Within the identify lifecycle, establish clear registration processes for NPEs. The rigor of the registration process should be dictated by the sensitivity of the data handled by a particular NPE.
    d. Determine the level of security protections (confidentiality, authentication, authorization) to be applied to unique data flows from NPE components.
    e. Establish clear authentication and authorization procedures for local access to NPEs.
    f. Define privacy protections required for different data categories. (Note: Establishing a framework reference definition for establishing privacy protections of Personally-Identifiable Information (PII) will aid in these definitions.)
    g. Determine and document whether outside organizations have access to certain categories of data.
    h. Define how to perform authentication and authorization for NPEs that are only intermittently connected to the network.
    i. Establish access control requirements that apply to NPEs according to the access control policies defined in the Identity Trust Framework.

Kantara Initiative. *Identity Relationship Management: Pillars of IRM*. https://kantarainitiative.org/irmpillars/
European Commission. 2012. IoT Factsheet – Identification. Report from the Internet of Things Expert Group (IoT-EG), Subgroup on Identification. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12
Internet Society. 2015. *The Internet of Things: An Overview*. https://www.internetsociety.org/doc/iot-overview

[5] The term "non-person entity" shall be used in this document in place of comparable terms currently in practice, such as "IoT devices," "digital entities," "digital objects," etc., in order to standardize reference terminology and remain consistent with FICAM/SICAM.

[6] International Telecommunication Union. 2013. *Recommendation X. 1255: Framework for Discovery of Identity Management Information*. http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en

2. Do not deploy NPE assets without changing default passwords for administrative access. If possible, do not deploy NPEs with only local access capabilities. Instead, attempt to integrate all NPE assets into the enterprise IdM system. (Note: This guidance does not apply to consumer-based NPEs that are attached to the enterprise network. New concepts similar to those required for bring-your-own-device (BYOD) registration of devices would need to be applied to that segment of NPE assets.

3. Evaluate a move to Identity Relationship Management (IRM) in place of traditional IAM, as recommended by the Kantara Initiative.[7] IRM is more suitable to NPEs than traditional IAM and is based on a set of pillars that include a focus on consumers and things over employees, Internet-scale over Enterprise-scale, and Borderless over perimeter. Identify and evaluate IRM vendor solutions as a possible fit for NPE identity requirements.

4. Design authentication and authorization schemes based on system-level threat models. Evaluate each individual NPE asset's implementation and choose vendors that have adhered to applicable standards and/or sought guidance or followed best practices from industry security groups. Take into account system vulnerabilities.

5. Smartphones for authentication on IoT. Mobile Devices and Telecommunication networks play a major role in the IoT. Smartphones will potentially be used as one means of authentication step to access things surrounding us. The features that makes the smartphone a powerful authentication factor needs to be tightly integrated with other devices. The next generation smartphones would drive different types of authentication mechanisms like facial recognition using the front-facing camera, voice recognition, gesture dynamics and handling dynamics in addition to traditional biometrics such as fingerprints. These smart phones could be used for enterprise level local authentication to IoT devices.

6. Create reference architectures for your NPE assets using *ITU-T Y.2060: Overview of the Internet of Things* as a starting point. NPE reference architectures enable consistent implementation of authentication, authorization, and accounting (AAA) services across all NPE assets in the infrastructure and can be used to test the overall access of systems at every level, from the individual machine to networks of machines at various layers in the technology stack. Identify the most vulnerable devices within the enterprise and apply MFA whenever possible.

7. Plan for the introduction of IPv6. Organizations have not fully moved to IPv6 as the industry is still in a state of prolonged transition. There are many NPEs that are designed to use IPv4, so planning now for how an NPE asset designed to use IPv4 will talk to an NPE asset designed to use IPv6, in a M2M implementation scenario, is needed. To make this feasible, consider a Software Defined Networking (SDN) mechanism that can allow these devices to talk to each other to provide the intended service.

[7] For more information in the Kantara Initiative's guidance on IRM, visit https://kantarainitiative.org/irmpillars/

8. Adopt a Public Key (PK) environment to support provisioning of certificates to NPE assets. The PK environment should implement certificate and cryptographic key controls consistent with Commonwealth Security Standard 501, NIST 800-53-5, or comparable certificate control framework.

9. Establish a plan for sharing NPE-related data with device manufacturers. Device manufacturers will continue to want to have device data access in order to monitor device health, track statistics, and be able to provide support to their customers. This data is collected and stored within various types of databases. Make sure to implement an authorization model for these back-end data stores such that 1) is compliant with relevant privacy regulations and 2) allows the minimal access required by manufacturers and other third parties.

10. Implement an AAA server that allow consumers to define preferences and provide services' consent for access to consumer profile data. An NPE implementation is one such service. This requires management of external identities such as consumers and patients, who are allowed to give their consent preferences for which attributes of their profile information can be shared and to whom. In many cases, this requires the integration of AAA services with third party services that manage consumer and business partner preferences for handling of data.

11. Consider integrating the identity management system with a building's Physical Access Control System (PACS) to enable additional security measures, such as selectively provisioning what doors and entrances a person's badge can access. These security enhancements will provide improved physical protection to NPE assets.

12. Implement restrictive logic in identity management workflows to proactively restrict access to NPE-related systems and devices if a person has not had the necessary prerequisites as specified by the access governance framework. Examples of prerequisites include training and background checks.

13. Implement a privileged user management system to ensure that administrators can access and monitor NPE systems and devices. This includes session monitoring of privileged sessions, protection of passwords to service accounts, and frequent password rotation.

14. Extend where possible the use of current asset management to inventory and document NPE assets. Categorize them based on risk and assign owners. Modify access records to support asset ownership, asset deployment, and any required revocation or asset lifecycle workflows. Integrate a service desk system that audits and automates the opening of tickets so that revocation of physical assets occurs in a system of record.

15. Invest in a well-documented plan for how to respond to failures and breaches when they occur. One example is an Incident Handling or an Incident Response plan. Note that this plan should be made a part of the incident management process and workflows.

16. Establish relationship mappings between people and NPE assets. This includes establishing explicit authorizations for people's authorized behavior on specific data sets. Enforce access management by both users and things. Implement MFA where possible for user access to NPE-centric data.

17. Develop effective AAA mechanisms for sensor nodes based on the context and service security requirements. Wireless sensor nodes can be a key element for NPE asset implementations; however, AAA of the sensor nodes in a wireless mesh network is not yet fool proof due to limitations in energy and computing power. Consider context as a way to determine the rigor of the authentication required based on risk introduced by a particular sensor node. Examples include location/coordinates, time-of-day, end-device/system being accessed, or data types being transmitted/received. Note: In some attack scenarios, context information is easily stolen, forged, or proxied. Also, evaluate the risk associated with context false-negatives and the potential risk that may result when legitimate users are incorrectly blocked (e.g., bad device clocks, upgraded endpoints, unexpected but legitimate locations, loss of GPS signal, etc). Perform threat modeling to determine the most appropriate AAA mechanisms for sensor nodes.

18. Leverage security controls built into standards-based NPE protocols such as CoAP, DDS, and REST to allow for interoperable authentication and authorization transactions between different manufacturers' NPE assets. A list of common NPE communication protocols and assertions has been provided in **Table 1**.

Table 1. Common NPE Communication Protocols and Assertions

Protocol	M2M Authentication Options	Description
MQTT	Username/Password	MQTT allows for sending a username and password, although recommends that the password be no longer than 12 characters. Username and password are sent in the clear, and as such it is critical that TLS be employed when using MQTT.
CoAP	Pre-Shared Key Raw-Shared Key Certificate	CoAP supports multiple authentication options for device-to-device communication. Pair with Datagram TLS (D-TLS) for higher level confidentiality services.
XMPP	Multiple Options Available Depending on Protocol	XMPP supports a variety of authentication patterns via the Simple Authentication and Security Layer (SASL – RFC4422). Mechanisms include one-way anonymous as well as mutual authentication with encrypted passwords, certificates and other means implemented through the SASL abstraction layer.
Zigbee	Pre-Shared Key	Zigbee provides both network and application level authentication (and encryption) through the use of Master key (optional), Network (mandatory) and Application Link keys (optional)
HTTP/REST	Basic Authentication (cleartext) (TLS Methods) OAUTH2	HTTP/REST typically requires the support of the TLS protocol for authentication and confidentiality services. Although Basic Authentication (where credentials are passed in the clear) can be used under the cover of TLS, this is not a recommended practice. Instead attempt to stand up a token-based authentication approach such as OAUTH 2
Bluetooth	Shared Key	Bluetooth provides authentication services through two different device pairing options, Standard and Simple Pairing. The Standard Pairing method is automatic; the Simple Pairing method includes a human-in-loop to verify (following a simple Diffie-Hellman exchange) that the two devices display the same hash of the established key. Bluetooth offers both one-way as well as mutual authentication options. Bluetooth secure simple pairing o-ers ‘Just works’, ‘Passkey entry’ and ‘Out of Box’ options for device-device authentication
Bluetooth-LE	Unencrypted data authenticated using Connection Signature Resolving Key (CSRK) Device Identity/Privacy is via an Identity Resolving Key (IRK)	Bluetooth-LE introduces a two-factor authentication system, the LE Secure Connections pairing model which combines – based on device capability – several of the available association models available. In addition, Elliptic-Curve Diffie Hellman is used for key exchange.

Source: CSA *Identity and Access Management for the Internet of Things – Summary Guidance*, pp 10-11.

Data Model for NPE Identity Information

The following data model for NPE identity information has been adapted from ITU *Recommendation X. 1255: Framework for Discovery of Identity Management Information.*

The data model for NPE identity information described in this section provides a uniform means to represent metadata records as NPEs, and can also be used to represent other types of information as NPEs. It is a logical model that allows for multiple forms of encoding and storage, and enables a single point of reference (i.e., the identifier) for many types of information that may be available in digital form.

Each NPE has an intrinsic set of attributes, a user-defined set of attributes, embodied in one or more elements and zero or more additional elements containing information such as text, video or images represented in digital form. All of these elements can be made available through a precisely defined NPE specification, which incorporates the capability for authentication using public key security, and perhaps other means of authentication using higher-level APIs, as might be implemented by NPE repositories. This provides access with privacy and security to NPEs.

The essential fixed attribute of a NPE is its associated unique persistent identifier, which can be resolved to current state information about the NPE, including its location(s), access controls, and validation, by submitting a resolution request to the resolution system. Examples of other intrinsic NPE element attributes are: date last modified, date created, and size. User extensible attributes may be set by the users with appropriate permissions.

Attributes that are not specifically addressed by the basic NPE data model include ownership, authentication and access terms and conditions. These attributes will be an important part of most NPE implementations; however, a single solution seems unlikely. Ownership and access control information will likely be contained in user extensible NPE attributes or in separate data elements. This provides a common way to deal with various ownership and information management schemes, as well as multiple authentication and authorization schemes, without making the assumption that a single approach will be used across all domains and user communities.

The combination of a standard data model, a defined protocol for interacting with that data model, and an identifier/resolution system, provides a key ingredient for the coherent long-term management of information in a digital context. The resolution system should be a distributed, secure, high-performance resolution system designed to enable persistent reference to digital entities over long periods of time and over changes in location, access methods, ownership and other mutable attributes.

The core capability for discovery of IdM information results from the use of the registry component, which includes the repository. The function of an individual registry is to federate across collections of NPEs, enabling end users and applications to search through and navigate the universe of registered entities.

Repositories that contain collections of NPEs can contribute metadata about the NPEs for which they are responsible to one or more registries. A single registry can collect metadata from multiple repositories, and a single repository can send metadata to multiple registries. The registries can provide search and reporting functions over the represented entities and provide an entry point into the structured world of NPEs and repositories.

There may be situations in which the registries are not, strictly speaking, needed, e.g., in the case where a direct reference to a NPE, in the form of its identifier, is embedded in another NPE or in a message or other document. In many cases, however, the end user, or automated process acting on behalf of a user, will not know the identifier to begin with, and will have to use some variety of search or sorting process to discover the needed reference. Even if a user knows the identifier, the user may not know how to resolve it, or how to interpret the resolution results. Recording the existence of NPEs in registries can help to solve that problem in a very general way.

By defining operations that interact with a specified data model, digital entities can be constructed and used to represent most types of structured information. A standard NPE data model has been illustrated in **Figure 1**. Representation of the entities in a form that is independent of the implementation details of the relevant storage system is an essential interoperability feature, as it allows multiple storage formats and approaches to be normalized to a single logical model.

Figure 1. Standard Data Model for NPE Identity Information

<table>
<tr><td rowspan="2"></td><th colspan="2">NON-PERSON ENTITY</th></tr>
<tr><th>ATTRIBUTE</th><th>EXAMPLE</th></tr>
<tr><th rowspan="3">Intrinsic Attributes</th><td>Unique Identifier (ID)</td><td>84321/ab5</td></tr>
<tr><td>Date Created</td><td>2016/02/10</td></tr>
<tr><td>Date Modified</td><td>2016/10/30</td></tr>
<tr><td colspan="3"></td></tr>
<tr><th rowspan="3">User-Defined Attributes</th><td>Object Type</td><td>89754/123</td></tr>
<tr><td>Permission Scheme A</td><td>84321/ab5</td></tr>
<tr><td>More…</td><td>…</td></tr>
<tr><td colspan="3"></td></tr>
<tr><th rowspan="4">Additional Elements (1-N)</th><th colspan="2">ELEMENT 1</th></tr>
<tr><td colspan="2">Intrinsic Attributes</td></tr>
<tr><td colspan="2">User-Defined Attributes</td></tr>
<tr><td colspan="2">Data</td></tr>
</table>

Source: ITU Recommendation X.1255, p. 9.

Except for the persistent identifier at the top, all data shown in Figure 1 is conceptual only. Each element of a digital entity can take different forms, i.e., digital entity references by identifier, an actual digital entity, plain local data suitably typed.

Registries may use or incorporate repositories to store metadata records; and repositories are information management systems that provide access to collections of NPEs via the digital entity interface protocol. Repositories may generally be thought to incorporate the digital entities to which they provide access. A more detailed view however, would show them as portals into various storage and information systems, mapping the raw data into digital entities that may be stored locally or remotely. This could be as simple as a file system holding the data for a given NPE in one or more files that are not known or visible to the user.

Alternatively, especially for complex digital entities, data may be spread across multiple locations and systems and brought together in NPE form only on demand, with one storage component holding the “map” of the entity and the bulk of the data held in other systems. This technique of interacting with existing systems is key to federation, as the information in an arbitrarily complex information system can be logically divided into NPEs, and those NPEs made available in a standardized fashion, using an instance of a NPE within user-centric applications.

A NPE client can locate one or more repositories for a given NPE by resolving its identifier. The resolution request will return the location of one or more relevant repositories with which the client can initiate a NPE transaction.

The NPE repository software normally provides multiple network interfaces for performing operations on digital entities, namely, the digital entity interface protocol for interacting with the NPE itself, as well as locally desirable interfaces as determined by current technology options. The various interfaces each have their own benefits in terms of security, compatibility with proxy servers and the use of ubiquitous client software. Redundancy is built into the digital entity interface protocol, along with strong individual and group authentication. Redundancy is supported by a mirroring system in which each NPE repository communicates with the others to ensure that replicated entities are kept in sync. Authentication is based on either secret or public/private keys or other authentication mechanisms.

Other notable features include replication, allowing easy mirroring across repositories and extensibility through a plug-in mechanism. Plug-ins could be built to manage both entity type specific activities, e.g., parsing a video format and dispensing a requested section, or activities oriented to network services, e.g., contributing metadata to a NPE registry.

8 IdM of NPE Use Case: Public Health Emergency Response

Purpose: To illustrate the complex challenges associated with IdM of NPEs across jurisdictions and domains of governance. An architecture model outlining the IdM and communications protocols required for the use case has been provided in **Figure 2**.

Use Case Scenario: Emergency response involving a biological hazard event within a populated urban area. Public health officials/NPEs must communicate with emergency management personnel/NPEs and hospital personnel/NPEs to address the public health impacts resulting from the biological hazard.

NPE Settings:

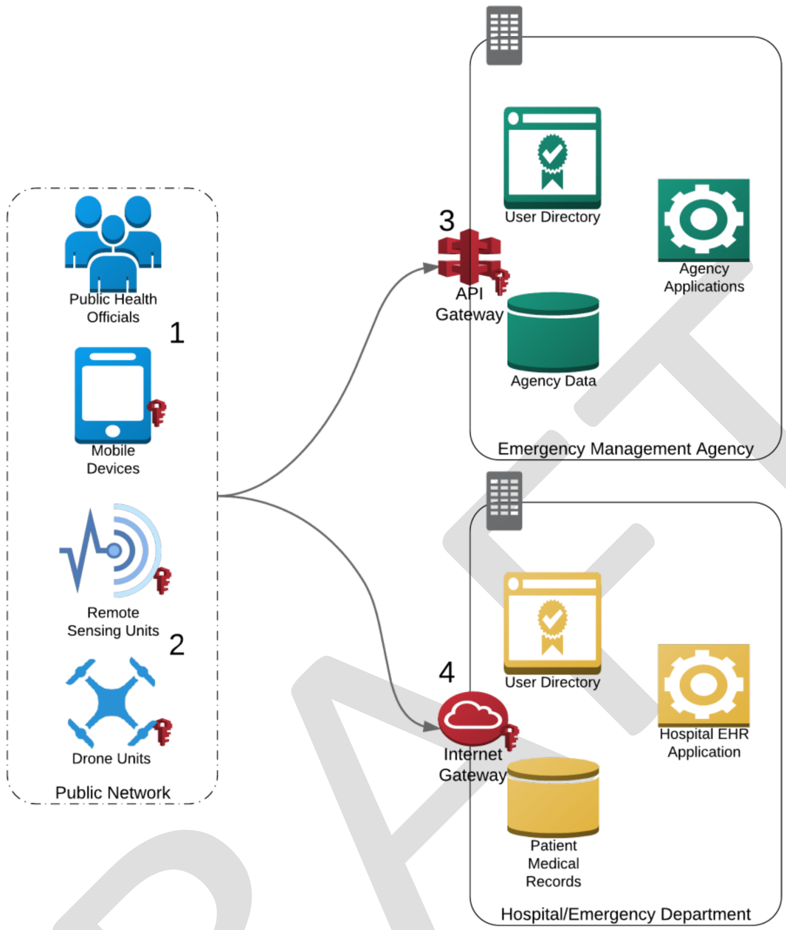
Human – NPEs attached to or inside the human body for vital signs
Hazard Site – NPEs for remote sensing of conditions in urban hazard zone
Vehicles – NPEs and applications/components within drone units
Supplies – NPEs delivered by drones, such as medications, and their tracking devices
Built Environment – NPEs for monitoring conditions in residential/commercial structures[8]

Runtime Flows (Figure 2):

1. Public health officials rely on authenticated NPEs for mobile communications and to monitor real-time feeds from remote sensing units to evaluate air, soil, and water conditions within the hazard zone – both in the outside and in the built environment (machine-to-machine).
2. Public health officials use authenticated drone technology to deliver medical supplies and measure vital signs of affected persons onsite (human-machine); IdM and data management must be compliant with the Health Insurance Portability and Accountability Act (HIPAA, P.L. 104-191) Security and Privacy Rules.
3. Public health officials authenticate to the emergency management agency's applications to submit data from monitoring activity (application/API).
4. Public health officials authenticate to a hospital's electronic health record system to submit patient-level data collected from persons within hazard zone in advance of transport to the emergency department (application/API); IdM and data management must be compliant with the Health Insurance Portability and Accountability Act (HIPAA, P.L. 104-191) Security and Privacy Rules.

[8] Internet Society. 2015. *The Internet of Things: An Overview*. https://www.internetsociety.org/doc/iot-overview
Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. 2015. *The Internet of Things: Mapping the Value Beyond the Hype*. McKinsey Global Institute. p.3. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

Figure 2. IdM of NPEs Use Case Architecture Model



Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council's membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit: https://vita.virginia.gov/About/default.aspx?id=6442474173