Subscriptionless Devices and Services

Alliance for Telecommunications Industry Solutions
October 2017

ATIS-I-0000061

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE : The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

1. Executive Summary

The emergence of Internet of Things (IoT)-based services is expected to create explosive demand for new devices and applications. Although a large percentage of IoT devices will ride Over The Top (OTT) of existing network subscriptions, many devices must still acquire network access from public (typically paid) Wide Area Networks (WANs) and, traditionally, must have a subscription with the network operator to do this.

This paper explores a variety of subscriptionless device models that benefit both the user and the network operator. For many IoT users, the direct IoT device connectivity subscription cost structure is often higher than the willingness to pay, given the utility of the device in question. Additionally, many end users have a desire to connect to their network of choice for "occasional" data without having to maintain an ongoing subscription. The subscriptionless device model can potentially reduce the cost and complexity for network operators as the network operator may not need to bear the full cost of maintaining "billions" of subscriptions for devices that may attach only occasionally to their network. Rather, operating models are described where the network operator's primary relationship is with a 3rd party authentication or application service provider instead of the device itself.

Some of the subscriptionless models are more naturally resistant to botnet security-related attacks and can provide an extra measure of security within the IoT context.

Although this paper considers the case for subscriptionless devices, this does not preclude the existence of a subscription with other 3rd party entities to facilitate proper charging and security for network services.

2. Introduction

2.1 Vision of IoT-enabled Market

IoT is the inter-networking of objects (both physical and virtual) with applications that enable application level control and/or monitoring of these objects. IoT objects can range from simple temperature or presence detectors to large vehicles or machinery. The ability to collect massive amounts of data from these objects while enabling control and management of remote objects opens the door to a wide range of new data-driven automation and efficiency-saving applications.

These new data-driven IoT applications and services will drive the proliferation of a wide variety of devices that will require network access. IoT services can provide significant advantages to consumers, enterprises, and government institutions.

Experts suggest that by 2020, approximately 30 billion IoT devices will be deployed worldwide.[1] These devices will be connected to the Internet or to private network environments and will need the ability to clearly assert an identity that can be authenticated by the network and/or application appropriate for that device. In some cases, the network operator's role in delivering IoT services is simply to provide connectivity and there is no direct technical or business partnering between the operator and the IoT service provider. In other cases, the network operator may take a more active role where the IoT service includes technical and business aspects under the control of the network operator. This whitepaper focuses primarily on the latter case, considering ways in which the network service provider can take better advantage of the transient revenue opportunities availed by IoT devices and applications while cost-effectively scaling the network to accommodate the potentially large number of IoT devices that require network services.

2.2 Low Data Rate, Low Connectivity (LDLC) Devices

A significant part of the IoT market that provides explicit network services to IoT devices can be characterized by many application-specific devices or clients that may only need to communicate on an "event" basis (potentially many days/months between events) with a small amount of data. These devices may only need to communicate in short bursts of data providing or receiving information on an "as needed" basis.

Examples can be found in both consumer and enterprise IoT markets.

Examples of consumer applications:

Unmanned Aerial Vehicles (UAVs) are often used in the consumer market for photography and other toy/hobbyist applications. These devices may require real-time control and monitoring functions to fly. However, the UAV itself may only be in operation for short periods of time limited by the battery life of the UAV as well as the

---

[1] *IEEE. Nordrum, Amy. "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated". 18 August 2016.*

leisure time available to the consumer to use the device. Based on seasonal variations, there may be long periods of time when these devices are inactive (e.g., the device may only be used during summer vacation periods.)

A variety of "Lost and Found" applications exist where the IoT networking function may only be needed when the object associated with the device needs to be located. For example, pet owners could equip their pet with a smart collar. If the pet should run off, an application may be invoked to locate the collar and thus find the pet. However, this application is not likely to be used very often in most circumstances.

Connected Car applications can include tracking, monitoring, and entertainment where the need is limited to specific events such as a vacation road trip or vehicle maintenance situation.

Seasonal home and property sensors are often needed to monitor property that is not personally attended to during an off-season. This monitoring may not be needed during active-use seasons.

Examples of enterprise and commercial applications:

UAV applications exist where a drone is used on an "as needed" basis for specific functions in specific areas. These applications may include construction inspection, field surveys, agricultural applications, and utility inspections. Often the device is only in use for a short period of time, for example, when the crop is nearly ready for harvest or just prior to/after construction of a structure.

In addition, a number of universities have initiated programs on drone journalism. Examples include:

- Drone Journalism Lab at the University of Nebraska-Lincoln's College of Journalism and Mass Communications, http://www.dronejournalismlab.org/.
- University of Missouri Drone Journalism Program, http://www.missouridronejournalism.com/.

These programs generally seek to create an interdisciplinary partnership dedicated to helping students understand and use UAV systems in service to society. Such programs will certainly help expand the set of UAV use cases in the future.

Similar situations exist for disaster-event field surveys, some insurance claim inspections, and first responder search-and-rescue operations.

For commercial vehicles and machines, the owner or manufacturer may want to periodically and remotely monitor the maintenance state to ensure safety.

Venue/Event management may use IoT devices during an event for real-time management of the event itself.

Many event-triggered remote sensors may only need to communicate once a day, week, or month with a short burst of data.

2.3 Subscriptionless Network Services & Devices

Current networks were built around stable, predictable, long-term revenue (subscription) models specifically optimized for high Available Revenue Per User (ARPU) devices. Examples include smart phone devices capable of providing the user with voice, messaging, and data/Internet services, as well as fixed-line data modems designed to handle the delivery of high-quality video and data service to multiple devices within a household or enterprise.

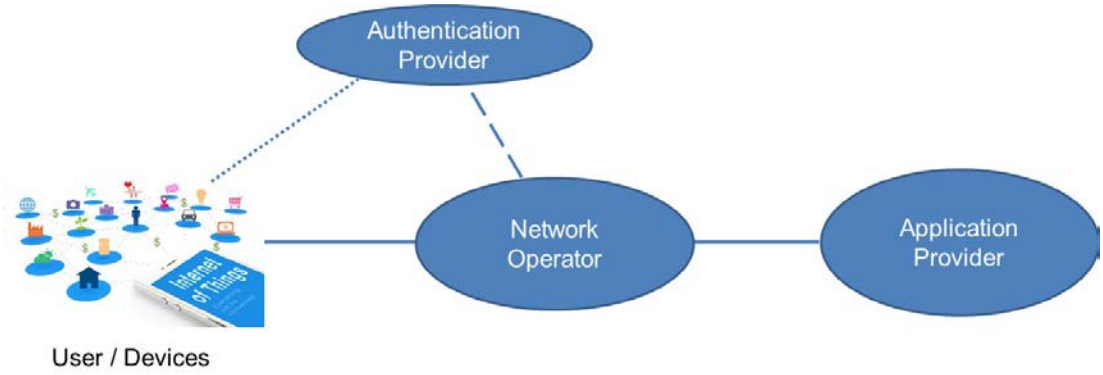
Although device-focused subscription-based models offer more predictable traffic profiles and simplified network management, these models do not address transient revenue opportunities efficiently. As noted in the previous section, the IoT market includes a wide variety of opportunistic applications that now require a network infrastructure that is sufficiently agile to capture these transient opportunities with minimal fixed costs.

This paper explores a class of network solutions where the network endpoint (device) acquires network services without having a subscription with the network service provider directly. These devices may have a subscription with a different network provider or 3rd party application service provider.

3. Key Players

There are two fundamental requirements for the provision of network services to a device:

- The network must be able to securely identify and authenticate that device onto its network to ensure the ability to properly manage the network.
- The network must be able to securely associate the device identity to enable charging for the network services provided.



There are 4 primary actors engaged in meeting the requirements noted above:

- The device intending to acquire the network service.
- The network operator providing the network service.
- An authentication provider who certifies the identity of the device given that the device does not have a subscription with the network.
- The application service provider who provides a service based on device communication.

3.1 Device/End User

The nature of the end device could vary from a small temperature sensor to a connected vehicle. Regardless of the form or level of sophistication, the assumption is the device does not have Wide Area Network (WAN) (e.g., Internet) access via nearby local networks. For example, the device does not have Wi-Fi or does not have the necessary credentials to authenticate onto a nearby Wi-Fi network that has Internet access. In order for the device to communicate to network servers, the device must then connect to a publicly accessible network such as:

- A public-licensed spectrum wireless network using standard 2G, 3G, 4G, or 5G radio technologies.
- A public-unlicensed spectrum wireless network provided by network operators, including service provider Wi-Fi and MulteFire-based networks.
- Other networks using various Low Power Wide Area Network (LPWAN) technologies.

In some cases, the device itself may connect to the WAN/Internet via an intermediate gateway device.

Since the device (or gateway element) will authenticate to a WAN, the device (or gateway element) should support secure storage and compute functions necessary for the management of credentials. This can be provided via a:

- Trusted Execution Environment (TEE) which provides a secure area from the main processor to provide confidentiality and integrity protection for code and data loaded inside the TEE. This provides an isolated execution environment to enable secure and protected cryptographic functions to run in support of credential management and authentication. The TEE specification is governed by the Global Platform (GP) industry association.
- Trusted Platform Module (TPM) which provides a standard, secure cryptoprocessor to secure hardware by integrating cryptographic keys, a capability to perform secure cryptographic operations using those keys, a capability that may be used for device authentication and attestation into devices, and a secure hardware-anchored credential that may be used for device authentication. The TPM technical specification is written by a computer industry consortium called the Trusted Computing Group (TCG).

Note that both of the methods referenced above can impose a high burden on small footprint, battery conscious IoT devices in terms of processing power, battery power, and complex functionality. However, the industry continues to pursue robust security measures which provide for a hardware-embedded trust-anchor for credential management. One such effort is the development of a Device Identifier Composition Engine (DICE), which provides for a secure hardware-anchored credential that may be used for device authentication and attestation.

3.2 Network Operator

The network operator provides a network service to the device and IoT application service provider. Typically, this service is a transport service of an object or set of data packets. However, other network services could be provided by the network operator such as location, paging services, or specialized routing services.

Since network operators must manage network resources to ensure effective and efficient usage, network connection privileges are often restricted to devices that meet certain network interface standards. In many cases, network operators may require appropriate compliance certification, or test to verify that a device will behave properly as a network connected device and has expected capabilities, including security capabilities/posture. However, for other devices, say for Wi-Fi network connections, device certifications are optional.

New network technologies such as Network Slicing[2] enable the network to apply different requirements on functionality such as charging, policy control, security, mobility, speed, availability, etc., to different network segments or slices serving different groups of devices with similar service/traffic characteristics. For example, subscriptionless services may require application-specific charging and policy control while other data transport use cases can efficiently be handled with standard charging or policies. In order to handle the multitude of segments and verticals in a robust way, there is a need to isolate the different segments from each other. For example, a scenario where a huge number of electricity meters are misbehaving in the network should not negatively impact the mobile broadband users or the health and safety applications. In addition, there is a need for independent management and orchestration of segments, as well as providing analytics and service exposure functionality that is tailored to each vertical's or segment's need. The functionality should not be restricted to providing isolation between different segments, but also allow an operator to deploy multiple instances of the same network partition.

These new network slicing capabilities allow the network to properly segregate subscriptionless device control, data, and management traffic to ensure that subscriptionless devices, which may not have undergone the same extensive certification

[2] *ATIS–I-0000050.v002, Section 5.1. "5G Reimagined: A North American Perspective (Issue 2)". February 2017.*

tests as standard network connected devices, can be sufficiently managed. The network slice model is well suited to subscriptionless services where the services of a network slice may be tuned and aligned with the large number of vertical applications or segments. The specifications for service access may then be aligned at the service level and micro-segmentation of services at a slice or sub-slice level to achieve the above mentioned objectives.

3.3 Authentication Provider

The authentication provider facilitates device authentication for service access on the operator network. The authentication provider's role may be viewed as similar to a Mobile Virtual Network Operator (MVNO) or the home network in an "always roaming" model. The authentication provider is responsible for ensuring that the network operator can validate the device credentials to authenticate the device onto the network. Examples of authentication providers include:

- A network operator (separate from the serving network operator) can offer outbound roaming services for its devices. Typical of roaming arrangements, the server network operator forwards device authentication credentials/protocol messages to the device's home network (the authentication provider) for authentication.
- A certificate authority can act as a trust anchor for a certificate. In this case, an authentication provider may acquire a certificate from the certificate authority to verify the identity of a device managed by the authentication provider. The certificate authority providing this certificate should be trusted by the network operator. The authentication provider can then install the certificate along with the associated private key in the device. Alternatively, the private key may be derived on the device and the public key is certified by the authentication provider. The device may then assert the certificate as part of the authentication procedure to the network operator for network services. The network operator can apply existing certificate management protocols (e.g., Online Certificate Status Protocol [OCSP]) to verify that the certificate is valid and has not been revoked.
- Federated authentication providers who can aggregate across multiple segments and many heterogeneous devices to provide an authentication and charging service to the operators. A variety of authentication

mechanisms may be used by the federated authentication providers to authenticate the device.

3.4 Application Service Provider

The application service provider provides application services using IoT devices. Applications typically run in servers in data centers with connectivity to the network operator. The application service provider generally has a strong relationship to the device. In this document, the application service provider is also referred to as the application provider.

In addition to authenticating with the network, an IoT device must also authenticate with an application server. As such, the application service provider must install, or derive and maintain, application layer credentials into the device to support application level authentication. These application level credentials may be completely independent from the network layer credentials. Additionally, unlike the network layer credentials which should be validated by a network trusted authentication provider, the application layer credentials, when provisioned by the application service provider, need only exist between the device and the application service provider.

4. Problem Statement & Business Drivers

As noted in Section 2, experts suggest that by 2020, approximately 30 billion IoT devices will be deployed worldwide, and as device numbers explode, the willingness to pay on a per-device basis decreases substantially. Indeed, when an IoT device is added to an existing local area network which has an existing network access subscription for Internet service, the network cost of the IoT device is often zero since the subscription is often sufficiently provisioned to handle a large number of low-data devices without increasing subscription levels. For example, a residential user with an unlimited 10 Mbps Internet service could add a large number of sensors, actuators, and other devices whose average data usage may be in the 10's of kbps. This similar situation also applies to enterprise networks. These environments create a user/enterprise expectation that network cost for IoT devices is nonexistent as the devices operate OTT of well-provisioned Internet services.

However, this situation does not exist for devices that are outside the domain of residential and enterprise local area network coverage. Section 2.2 illustrates a wide variety of applications where the IoT device is not able to ride OTT of an existing network

subscription. These devices must acquire network access from public (typically paid) WANs, and traditionally must have a subscription with the network operator and often an access-specific secure authentication mechanism.

The problem arises in that the direct IoT device connectivity subscription cost structure is often higher than the willingness to pay, given the utility of the device in question. For end users, there is desire to connect to the network of choice for "occasional" data without having to maintain a costly subscription.

To serve this class of device/user, network operators are faced with a fixed-cost network that has often been optimized for high-value subscriptions for smartphones (and other smart devices such as tablets), and high-bandwidth video appliances. To better serve this class of IoT devices, the network cost structure needs to be much lower and better optimized to address a much larger set of low-bandwidth, low-usage devices. There are a number of network structures a service provider can use to better optimize its network. In some cases, network operators have deployed a bespoke network access infrastructure to address low data usage devices. This paper considers additional ways for the service provider to minimize fixed costs in the network by eliminating the need to acquire, provision, and maintain subscription data/profiles in the network for billions of devices while still meeting basic network needs.

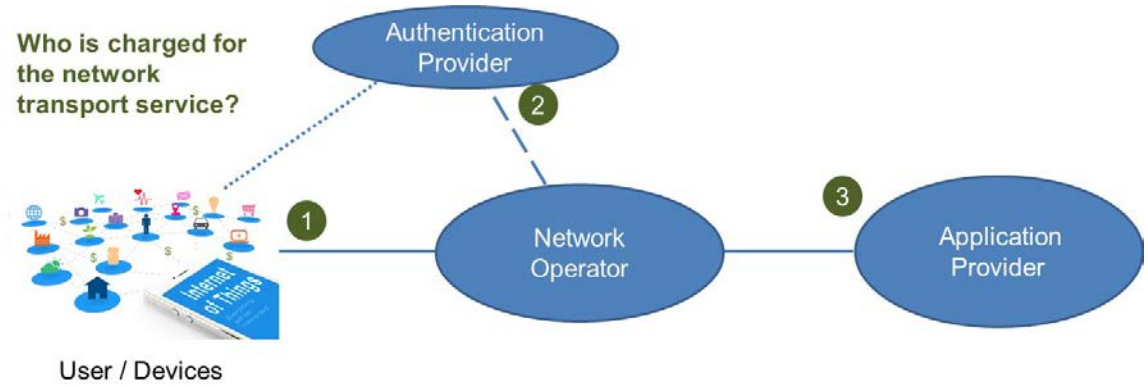
Of course, in all cases, the network operator will need secure device credentials to authorize a device onto the network, and will need assurance that an appropriate entity can be charged for any network service provided.

Although this paper considers the case for subscriptionless devices, this does not preclude the existence of a subscription to facilitate proper charging for network services. For example, options exist where a 3rd party subscription (e.g., to an application provider or authentication provider) can be used for the delivery of network services to subscriptionless devices. These and other charging examples will be discussed in more detail in the next section.

Additionally, network support for subscriptionless devices can benefit 3rd party actors such as application providers or authentication providers. It is important to note that the large majority of IoT devices will be short-range non-cellular devices connected by unlicensed radio with a typical range of around 100 meters, such as Wi-Fi, Bluetooth, and ZigBee, or over fixed line local area connections. Some estimates indicate that by 2022, 16 billion devices will exist in this class, whereas 1.5 billion IoT devices will connect via

cellular networks.[3] With less than 10% of IoT devices connecting directly to wide area mobile networks, application providers may find it attractive to utilize the same security mechanism they use at the application layer to also provide network access (possibly using derived keys or bootstrapped application layer credentials).

5. Deployment Models & Options



In the figure above, the network operator can provide a network service to a device, such as transporting data objects between the device and an application provider. In providing this service several basic actions must take place, including:

- The device must attach to and securely authenticate with the network (1). The network may utilize a 3rd party authentication provider (2) to verify the identity and authenticity of the device. The network operator may also choose to segregate this class of devices into a separately managed network slice.
- The network facilitates communication services between the device (1) and an application provider (3).
- The network operator collects charging information and identifies the appropriate party to be charged for the service.

In this configuration, three possible actors could be charged for the network service:

[3] *Ericsson. "Internet of Things Forecast," August 2017.*

1. The device itself could pay in real time for the network service.
2. A 3rd party authentication provider with an association with the device could be charged for the network service.
3. The application provider associated with the device could be charged for the network service.

5.1 Authentication Models & Methods

Prior to the delivery of a network service to the device, the device must connect to the network. The network operator must maintain the integrity of their network and as such, connection services are only offered to devices with trusted credentials. Specifically, the device should have:

- A globally unique identifier.
- Strong credentials associated with the identifier that can be trusted by the network operator.
- A mechanism to identify which party can be charged for the network service provided.

A globally unique identifier is needed since it highly desirable that the device can authenticate with as many network operators as possible worldwide. There are many possible mechanisms that could be used to create a globally unique identifier. For example:

- The International Mobile Subscriber Identity (IMSI) is usually presented as a 15 digit number. The first 3 digits are the Mobile Country Code (MCC), which are followed by the Mobile Network Code (MNC) of 2-3 digits. The remaining 9-10 digits are the Mobile Subscription Identification Number (MSIN). Since IMSIs depend on registered mobile country and network codes, they are generally reserved for network operators. Additionally, a 9-10 digit MSIN will create scalability issues as the number of IoT-connected devices expands into the billions worldwide.
- The Network Access Identifier (NAI) is a standard way of identifying users who request access to a network. The typical syntax is "user@example.com". Since example.com can be a uniquely registered domain name, the resulting NAI can be globally unique.
- oneM2M App-ID is a globally unique identifier of the form R<registration authority>.<reverseDNS>.<appName>. This App-ID could be used to

create device specific globally unique identifiers of the form <App-ID>.<device serial number>.

In addition, the identifier must be presented as a set of security credentials to enable secure authentication of the identified device by the network operator or the authentication provider. A number of options exist, including:

- Use of a Pre-Shared Key (PSK) mechanism for authentication. In this case, a key associated with the identifier is either provisioned into the device prior to deployment or provisioned after deployment as part of larger security framework. The key would also be held by the authentication provider. This mechanism includes existing 3GPP Authentication and Key Agreement (AKA) and Generic Bootstrapping Architecture (GBA) authentication mechanisms.
- Use of a device certificate. In order to ensure that the certificate can be trusted by network operators, the operators can choose to create a governance authority and associated policy administrator to manage certificates that can be trusted for network access. In this way, the governance authority/policy administrator can certify a list of trusted certificate authorities that can be used to create certificates that can be trusted by the network operator for device connection purposes.

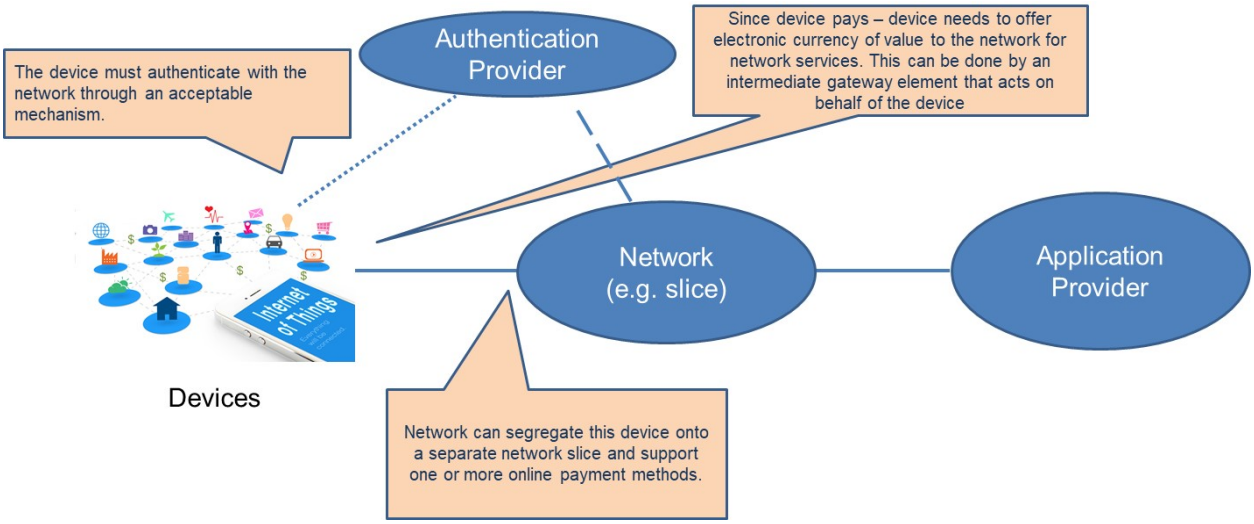
Finally, the authentication process must provide sufficient information to the network operator to enable charging of the correct party (authentication/application provider) for network services rendered to the device. This can be done in a variety of ways, including:

- Since the globally unique identifier has a component that is registered (e.g., a oneM2M Application ID), the registration database could be queried to identify the entity to be charged.
- If a certificate is used, the certificate can include sufficient information to identify the entity to be charged.

5.2 Device Pays

As noted earlier, many devices do not have a separate network subscription and do not need to pay for transport since they ride OTT of other subscriptions (e.g., via Wi-Fi). This

covers devices in the home (which may ride OTT of home Wi-Fi), devices in the enterprise, and for many industrial applications. As such, this section considers the class of devices "out in the wild" where access must be procured from a commercial mobile/wireless network.



The capability for a device to pay, in real time, with online electronic currency, is available in the Wi-Fi domain, as well as for selected scenarios in licensed spectrum. In these cases, the network might redirect the device to an online portal to allow the user to submit payment directly or indirectly for network access. This capability requires the user to manually interact with the portal, making this technique less applicable to the IoT domain where the device is not typically directly operated by a human user. Nevertheless, there are a variety of mechanisms that could potentially be developed for an IoT device to directly, in real-time, pay for a network service. For example, mechanisms might be developed that could allow the device to use:

- Automated distributed electronic payment systems such as bitcoin to pay for a network service.
- Other automated online payment mechanisms, such as a token that can be cashed in real-time by a network operator with a centralized authority to address double spending issues.

For 3GPP networks, these potential methods could require changes in the network charging infrastructure. Although existing online charging capabilities have been defined in 3GPP for mobility systems, new functions would be required to offer a real-time payment capability to the device, and provide the necessary logic to verify payment and

interwork with the existing 3GPP Online Charging System (OCS). For example, in the case of token-based payments, functions would be required to assign a payment token, evaluate the token for remaining balance, and authorize/reject access.

A detailed discussion of device online payments will not be addressed in this document as the scope of this document is focused on system and network authentication architecture aspects, not the charging architecture impacts. It should be noted that the potentially high transaction cost of many of these conceptual payment methods does create challenges. The actual charge for the transport of an object of data may be quite small, much less than a U.S. Dollar. Yet transaction costs of credit cards are well known and even bitcoin transaction costs have increased to over $2 in the U.S. in 2017[4].

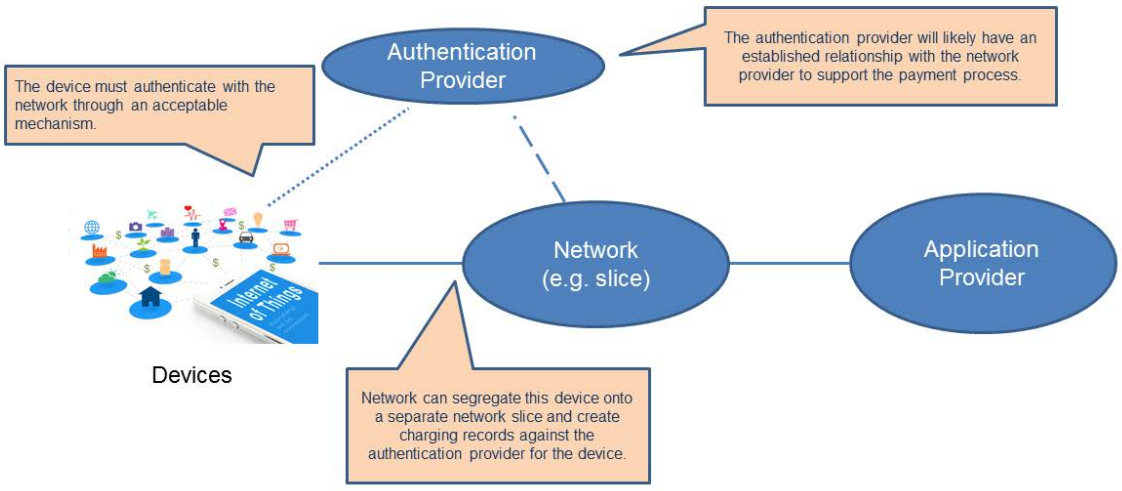
Additionally, online direct payment methods do require a high level of device intelligence and sophistication. Devices must be able to securely acquire, store, and distribute electronic currency to utilize this method of payment. Nevertheless, devices could connect with the assistance of a delegated application service provider or through a Customer Premises Equipment (CPE) gateway element which may include the necessary intelligence and capabilities to negotiate payment for network services on behalf of the device.

5.3 Authentication Provider Pays

The case where an independent authentication provider pays for the device network service is equivalent to the normal roaming model commonly used today.

As before, the device must securely attach and authenticate to the network. Authentication would typically be provided through an independent authentication provider which would also be charged for the network service provided.

[4] *Bitcoin transactions costs can be calculated by looking at the current average transaction costs from https://bitcoinfees.21.co/ and converting this to U.S. dollars (or other currencies) at http://www.btcsatoshi.com/.*



5.4 Application Service Provider Pays

As illustrated in Section 2.2, a large number of IoT device types are strongly associated with an application. Since networks generally provide network firewalls that prevent communication not initiated by the device, an application server can provide notification and other access services to devices. Additionally, IoT devices often rely on the application domain to provide the end service to a user leading to a strong, mutually authenticated security relationship between the device and application provider. Scenarios where this natural relationship between the device and application can be leveraged for the acquisition of network services can exhibit added efficiency. Examples of mechanisms that may be used include bootstrapping procedures whereby access layer and/or application layer credentials may be used to enable authentication at any of the layers.

In this scenario, both the network operator and application provider benefit in a number of ways:

FOR THE APPLICATION SERVICE PROVIDER:

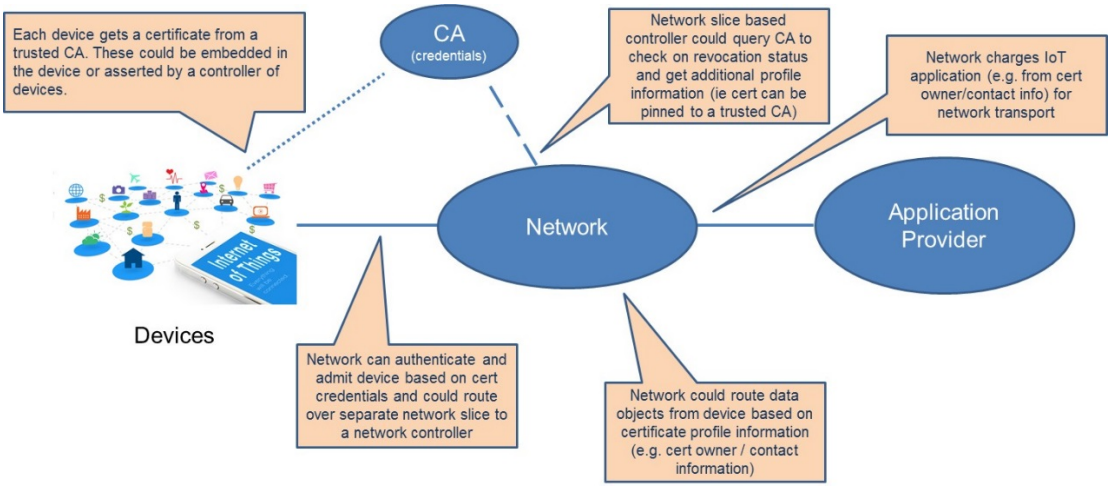
- The security mechanism used for their device ecosystem can now also be leveraged for public network access.

- The application provider can use the same credentials (e.g., a certificate) to attach with any number of different network operators, which may depend on business policies rather than technical considerations.
- The application provider creates an access environment with strong security attributes and in particular, enhanced resilience to botnet infections.

FOR THE NETWORK OPERATOR:

- The network operator no longer bears the fixed cost of maintaining "billions" of subscriptions for devices that may attach to their network.
- The network operator encourages new business relationships with application providers and thus maintains many of the advantages of a subscription-based service without the per-device subscription overhead.
- The network provider can play a key role in providing botnet security mitigation services.

A pictorial illustration of this scenario is shown in the figure below.



For illustrative purposes, the example shown in the figure above assumes the application provider has acquired a device certificate from a Certificate Authority (CA) that is trusted by network operators. Other authentication mechanisms are possible as discussed in section 5.1. The device then uses these credentials to attach and authenticate to a network operator. The network operator could segregate this device into an

independent network slice for security purposes. Once authenticated, the network operator identifies the application provider either through the authentication process or via a profile associated with the authentication process. Traffic from the device can then be routed and charged to the appropriate application provider. A more detailed description of this scenario is included in the Appendix.

Another possible scenario is where the application provider assures trust in the device to the operator. A global identity or decorated ID, which includes the application provider identity, can act as a gating and routing point for initially directing and allowing a device to attempt an attachment with the network. The network operator's trust in the application provider enables authentication, authorization, and derivation of access layer credentials which are then used by the device. The network operator identifies the application provider early in the attachment process even before the device completes authentication with the network. Once the device is authenticated, traffic from the device can be routed and charged to the appropriate application provider.

5.5 Network Integrity

As a result of the high value associated with licensed spectrum, network operators take extra care to ensure that licensed spectrum devices are certified to behave properly on their networks. The same care may need to be applied to subscriptionless devices operating in licensed spectrum. Given the large diversity and variety of devices expected to be deployed, the traditional certification model (e.g., Common Criteria, CPA) can be very costly for an operator.

Subscriptionless device certification can take many forms and be communicated in many different ways. For example, modern licensed air interfaces (such as LTE and the 5G NR) are complex systems that today are only supported by a small set of chipset vendors with a limited number of chipsets. Given that many IoT devices only require limited capabilities, it may be possible to certify based on chipset and the associated firmware version.

A multi-layer certification, when implemented properly, may significantly simplify verification of security capabilities/security posture of subscriptionless devices, allowing them to be more thoroughly vetted for the network access, e.g., a wireless System on a Chip (SoC) may be evaluated and certified independently. If this SoC is then used in a device, then a higher degree of confidence in the device is achieved by virtue of the device using the specific SoC.

Additionally, a 3rd party certification authority could provide certification services for devices.

In either case, the device could present a signed certificate to the network indicating its level of certification during the authentication process. If the device authentication is performed through the use of a trusted Public Key Infrastructure (PKI), the network operator governance authority can place as a requirement for issuance of a device certificate, a condition of certification (e.g., certification level). In this case, the device certificate used for authentication can also provide trust assurance based on the certification level.

An analysis and recommendation of device and network certification options is a matter for future study and is not within the scope of this document.

6. Assumptions & Areas for Future Study

6.1 Device Considerations

Throughout the document, device capabilities are assumed to exist even though these capabilities may not be available or deployed in networks today. General device assumptions include:

- Devices could be either 3GPP compliant or non-3GPP compliant.
- Devices may be aggregated using a gateway function that provides the interface to the network operator. In this case, the gateway element is "the device" from the perspective of the network operator.
- Devices have sufficient compute power to support secure authentication and transport capabilities.
- Devices may use either licensed cellular bands or unlicensed spectrum. Unlicensed air interface protocols could include Wi-Fi, LoRa, MulteFire and other standards designed for unlicensed usage.
- Devices can support a variety of network authentication mechanisms.
- Devices (particularly licensed spectrum devices) may require some level of certification and secure device identification.

Today, 3GPP devices utilize the AKA protocol run typically from a Universal Subscriber Identity Module (USIM) on a smart card (called a Universal Integrated Circuit Card [UICC]). AKA is a challenge response-based mechanism that uses symmetric

cryptography, not public/private key cryptography associated with certificates. However, new 3GPP 5G specifications in TS22.261[5] include a number of requirements related to authentication of 3GPP devices. Specifically, Section 8.3 of TS22.261 indicates that the 5G system shall support operator controlled alternative authentication methods (i.e., alternative to AKA) with different types of credentials for network access for IoT devices in isolated deployment scenarios (e.g., for industrial automation). As such, it is reasonable to assume non-AKA methods will be supported at some point for 3GPP IoT device applications.

Topics such as paging for subscriptionless devices require additional analysis and are left for future study.

6.2 Regulatory Considerations

The use of subscriptionless devices raises a number of regulatory questions; particularly in the area of privacy and legal intercept. These questions are topics for further study.

Privacy

Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.

It is clear that privacy applies to an individual or a group of individuals and not to inanimate objects such as light poles, drones, etc. However, quite often, many inanimate objects (e.g., cars, drones, medical devices) are extensions of individuals or groups and can disclose private information about them. Privacy of permanent identifiers (be it a device, network, or application identifiers) can be difficult to achieve. When done incorrectly such lack of identifier privacy protection can lead to disclosure and tracking of location, habits, etc., of individuals, leading to cyber and sometimes to kinetic attacks. 3GPP networks generally require identifiers such as the International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI) to remain private within the access network. However, as new authentication methods are supported for

[5] *3GPP TS 22.261, "Technical Specification Group Services and System Aspects; Service requirements for the 5G system".*

networks, it is unclear how, and whether, privacy protection can be achieved for the identifiers associated with subscriptionless access.

LI Considerations for Subscriptionless Access

Lawful Interception (LI) refers to the facilities in telecommunications and telephone networks that allow law enforcement and intelligence agencies with court order or other legal authorization to selectively wiretap individual subscribers. Most countries require licensed telecommunications operators to provide their networks with legal interception gateways and nodes for the interception of communications.

Similar to privacy, it is unclear how, and whether, legal intercept can be realized for subscriptionless access.

7. Summary

The current IoT device connectivity subscription cost structure is often higher than the willingness to pay given the utility of the device in question. Additionally, end users have a desire to connect to the network of choice for "occasional" data without having to maintain an ongoing subscription. Furthermore, the introduction of a multitude of network applications and segments together with the wide diversity of device types that may attach to the operator network poses a management burden and a threat to the operator networks. This paper considers ways for the service provider to minimize fixed costs in the network by eliminating the need to acquire, provision, and maintain subscription data/profile in the network for billions of devices while still meeting basic network connectivity needs for security and integrity.

There are two fundamental requirements for the provision of network services to a device:

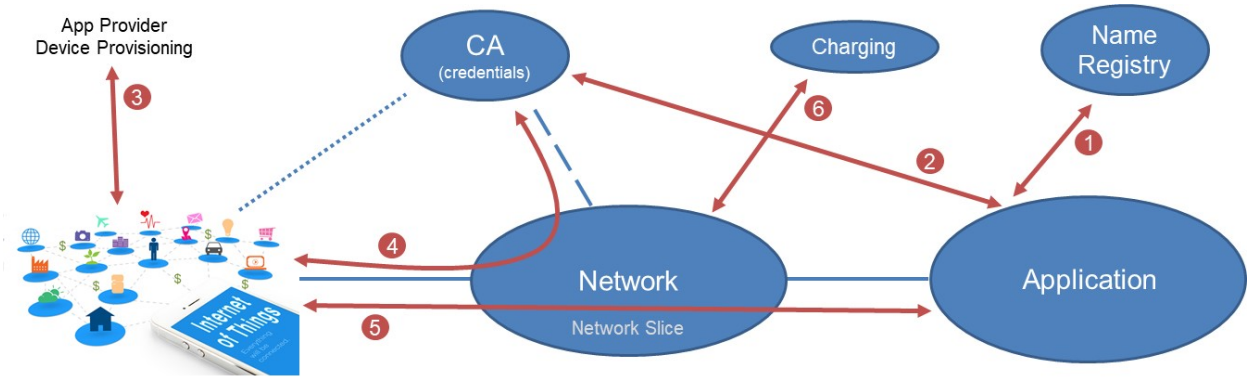
- The network must be able to securely identify and authenticate that device onto its network to ensure the ability to properly manage the network. Authentication of the device may go beyond traditional credential-based authentication and include additional assurances through device certification, that once the device attaches to a network, it will behave as expected.
- The network must be able to securely associate the device identity to a responsible party to enable charging for the network services provided.

Within this context, this paper has explored a number of ways for the network operator to securely authenticate a device while ensuring that any network services provided to the device can be properly charged. Specifically, the paper reviews how 3rd party authentication mechanisms can be used to securely authenticate the device. In addition, charging models are discussed which would allow the network operator to charge the device, a 3rd party authentication provider, or an application provider for network services rendered.

APPENDIX – Network Scenarios Where the Application Service Provider Pays for Network Services for a Subscriptionless Device

Although many possible configurations exist where an application provider can pay for network services for their devices, example scenarios are described below for illustrative purposes. The first example assumes a PKI is used for authentication.

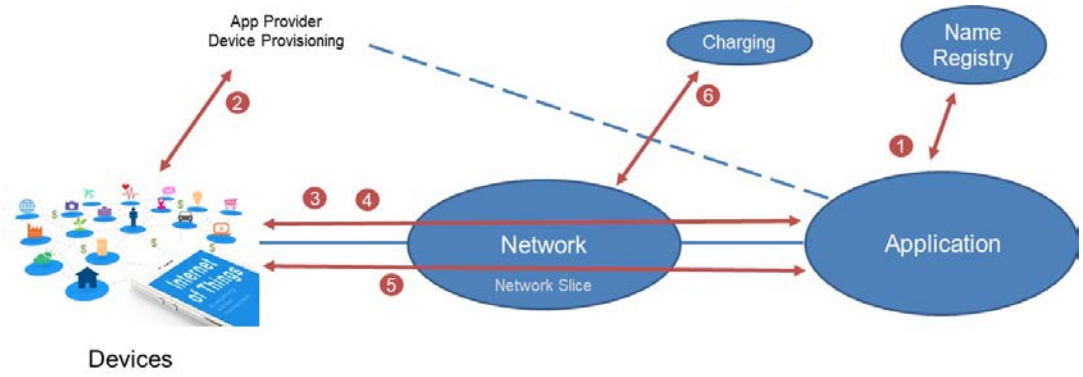
Consider the situation where the application provider acquires a per-device certificate to strongly authenticate the device to the application at the application layer.



1. The application provider has registered a root name so that a globally unique identifier can be assigned to the device.
2. Given a specific authenticated device to be used, the application provider can establish credentials for the device and acquire the certificate from a well-known CA that is approved and trusted by a set of network operators in accordance with rules established by a network operator certificate governance authority and associated policy administrator.
3. The application provider device-provisioning system can then provision application credentials onto the device or derived credentials for the device and install the certificate.
4. After being placed in service, the device can initiate attachment procedures to attach (connect) to one of the network operators in the set of network operators noted above.
    - The network operator accepts the device attachment request.

        - Validating the certificate signature and ensuring the device possesses the private key associated with the certificate using standard certificate based authentication methods. The network operator can also verify that the certificate has not expired or has been revoked.
        - After validating the application provider, as provided in the presented identity, and the existence of a service relationship between the network operator and the application provider, the application provider may assist in authentication of the device. After successful application authentication, the application provider may provide the network operator with a token comprising a session credential which may be used by the operator to complete the device-to-network authentication and attachment.
    - The network operator could then associate this device to a network slice sufficiently segregated from other network functions to assure some level of security and trust.
    - The network operator may make network attachment contingent on the existence of a business relationship between the network operator and the application provider to which the identity/certificate is registered.
5. Once attached, the network operator can provide packet/object transport services:
    - These transport services could leverage Virtual Private Network (VPN) services between the network operator gateway and that application provider. In this way, the services could be provisioned such that connectivity is exclusively between the device and application, thus mitigating the possibility of participation in botnet activities.
    - These network services could also leverage name-based network constructs for additional fine-grained routing to specific servers within the application provider domain.
6. The network operator creates charging records for all network services provided to the device or to the application provider for communication to the device for the purpose of upstream billing of the application provider.

The following example is very similar to the above scenario except a per-device certificate is not utilized. Instead, the application layer device credentials are used (e.g., via a token) to enable the device to receive services from the network operator. As in the scenario above, a business and service relationship exists between the network operator and the application provider:



1. The application provider assigns a unique global identity to the device, which incorporates a reference to the application provider identity to aid in discovery of the application provider.
2. The application provider then authenticates the device and provisions the global identity and credentials onto the device.
3. After being placed in service, the device can initiate attachment procedures to attach (connect) to one of the network operators in the set of network operators noted above.
    - The network operator receives the global identifier from the device in an attachment request.
    - The network operator validates the identity of the application provider presented in the global identifier and the existence of a business and service relationship between the network operator and the application provider.
    - After validating the application provider, the network operator reaches out to the application provider to assist in authentication of the device.
    - The application provider completes application layer authentication of the device with the assistance of the network operator.
    - The application provider may then provide the network operator with an authorization token comprising a network access session credential, which may be used by the network operator to complete an access layer authentication with the device.
4. The network operator may then complete attachment of the device and associate the device to a network slice that is sufficiently segregated from other network functions to assure some level of security and trust.

Steps 5 and 6 are the same as for the first example.