FILAMENT

Foundations for the Next Economic Revolution

Distributed Exchange and the Internet of Things

Executive Summary

As more and more devices are connected in the Internet of Things (IoT), an enormous amount of value is waiting to be unlocked. To make that possible, Filament has built an open technology stack that leverages the most advanced communication and security methods available today and thus enables devices to discover, communicate, and interact with each other in a fully autonomous and distributed manner.

Filament technologies provide a secure foundation for decentralized interaction and exchange.

Consider a deployment on a rail network, in which locomotives, freight and passenger cars, switch motors, and other pieces of infrastructure are networked through inexpensive, surface-mount devices such as Filament Taps. Suitably designed, such devices can communicate with each other over radio (as Taps do) instead of relying exclusively on WiFi, cellular, or satellite access. Now the rail network can gather realtime data from all of these devices under a variety of network conditions, devices can respond in real time, upload the data to run preventive analytics,

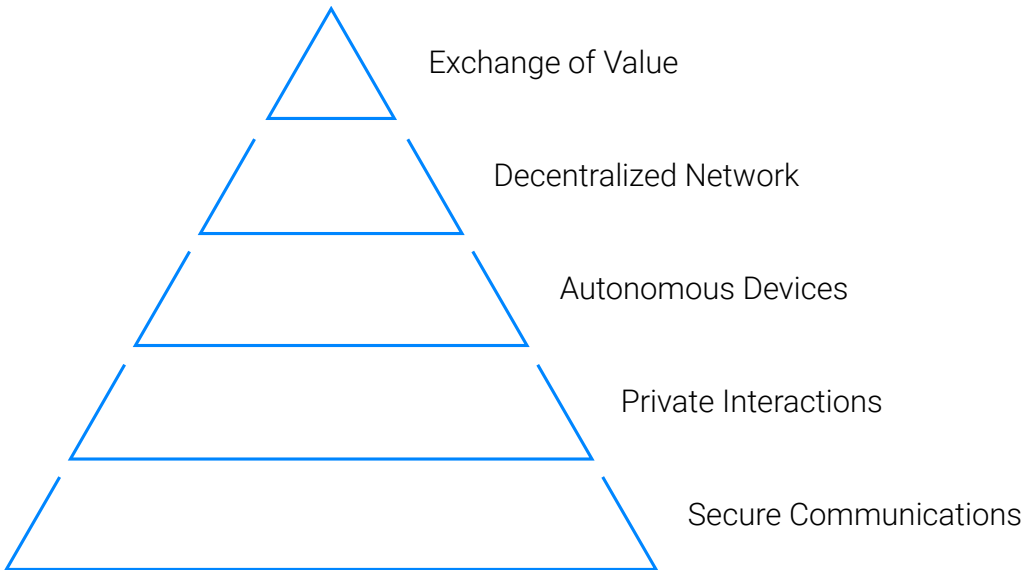
perform more targeted maintenance, and reduce the risk of dangerous and costly derailments.

In addition, the devices involved can exchange value directly or indirectly with a wide range of entities. For example, they could sell data about environmental conditions to a meteorological agency, sell data about usage of the rail network to an organization specializing in business statistics, sell access to their private communication network to customers along rail routes such as grain elevators and loading docks, or sell access to the rail cars directly. As these examples indicate, the exchange of value is not limited to a single location or vertical but can cross organizational lines in secure and flexible ways.

As explained in the remainder of this white paper, all of these interactions are made possible by hardware and software technologies that put a premium on security, privacy, device autonomy, fully decentralized communication, and the free exchange of value.

The SPADE Framework

The Filament technology stack is built upon five key principles: Security, Privacy, Autonomy, Decentralization, and Exchange (SPADE). These principles are additive (e.g., interactions can't be private if communications aren't secure, and the direct exchange of value is enabled by autonomous devices).



Security

Secure technologies guarantee that information is not disclosed to unauthorized entities (confidentiality) and not modified in an unauthorized or accidental manner (integrity). Security often involves encryption: encoding information so that only authorized entities can decode and thus understand it. The most common Internet technology for security between clients and servers is Transport Layer Security (TLS, Dierks and Rescorla 2008, RFC 5246). Although SSL/TLS is also used in IoT applications, more specialized protocols can provide the same security benefits with a great deal less complexity, using the most recent advances in cipher suites and forward secrecy.

Privacy

As the Internet threat model has changed, privacy has become a more important consideration for communication technologies (Cooper et al. 2013, RFC 6973). At root, privacy involves the protection of information about interactions, as opposed to the interactions themselves. Such information (often called "metadata") might enable an attacker to correlate interactions with a particular individual, analyze the traffic generated by an endpoint, uniquely identify or "fingerprint" a device, or otherwise detect the identity or attributes of an entity. Privacy-respecting technologies prevent attackers from learning such information, for example by using ephemeral addresses or routing data over ad-hoc links.

Autonomy

On the traditional Internet, the only "first-class" citizens are services associated with domain names. Individuals register accounts to become users of such services, and users can in turn authorize particular devices for use with their accounts. This pattern is apparent in, for example, the address format for XMPP: account@service/device (Saint-Andre 2015, RFC 7622).

At Filament, we instead treat devices as primary. The devices affixed to the cars of a freight train should not need to call out to a centralized service in order to communicate with each other or with the head-of-train device in the locomotive. They should have the ability to establish direct channels with any type of device at will.

Once we start to think of devices as autonomous agents that can interact with each other directly and independently, many powerful analogies for economic interaction become relevant. We can apply a wealth of societal and legal context that has been built up over thousands of years, such as contracts, double-entry bookkeeping, and escrow arrangements.

Decentralization

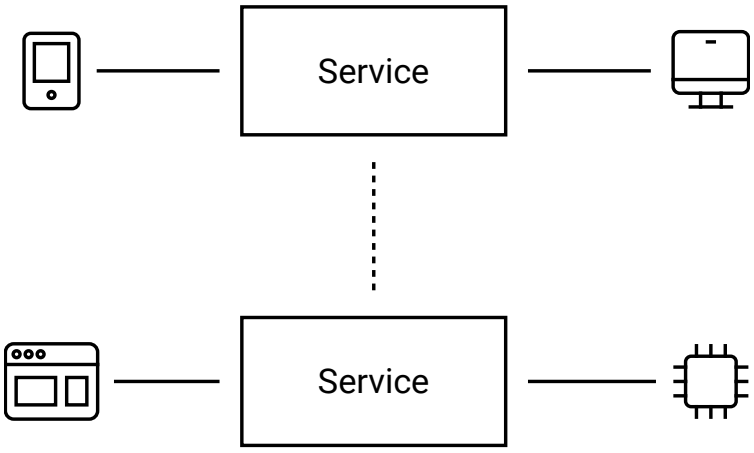
The autonomy of devices leads directly to a more decentralized architecture, meaning there is no single central authority that regulates or makes decisions for all the actors on given network.

The popular services of today are monocentric: Twitter, Facebook, WhatsApp, LinkedIn, and all the rest. Endpoints and their data are tied to each service, and the services do not talk to each other.

Monocentric Networks

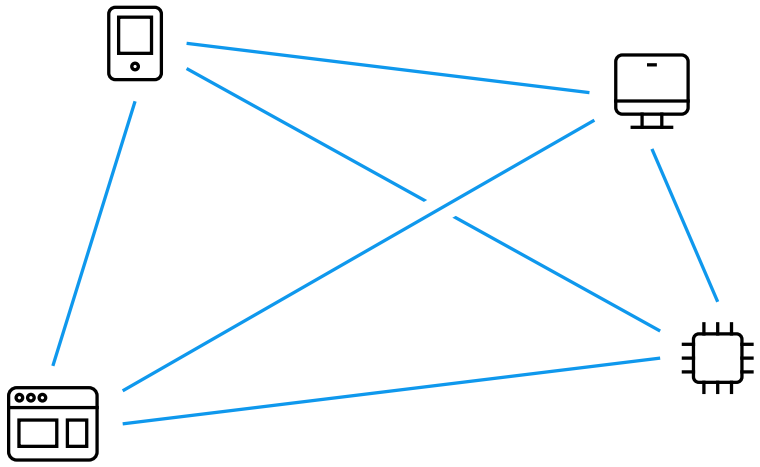
Technologies like email and Jabber/XMPP are polycentric, in that anyone can run their own service on a federated network where services talk to each other; however, these technologies still assume that services are primary and endpoints are secondary.

Polycentric Networks



By contrast, autonomous endpoints can create their own networks simply by interacting with each other directly, thus building up completely decentralized architectures of communication. This is important for devices in remote locations, but it is also the key to unlocking value from device-to-device interactions (e.g., because the intercession of a service might increase transaction costs beyond the point of viability).

Decentralized Networks



Decentralized architectures also improve the security profile of deployments, since there are no accounts to be hacked and no single point of failure at which a denial of service attack can be launched.

Exchange

The foregoing foundations enable us to build new models of device-level exchange. The values exchanged here could be data, network access, currencies such as Bitcoin, compute cycles, contracts for ongoing service, trusted introductions to other devices, and much more. At Filament we have not even attempted to define a taxonomy of such exchanges because we recognize that these values will emerge over time through countless interactions among devices. However, we have built the scaffolding for such interactions through primitives such as smart contracts and microtransactions.

Core Features of Filament Technologies

The SPADE design criteria animate all of the core features of the Filament stack: communicating with other devices, discovering their identities and capabilities, negotiating interactions, and finally exchanging value.

Communication

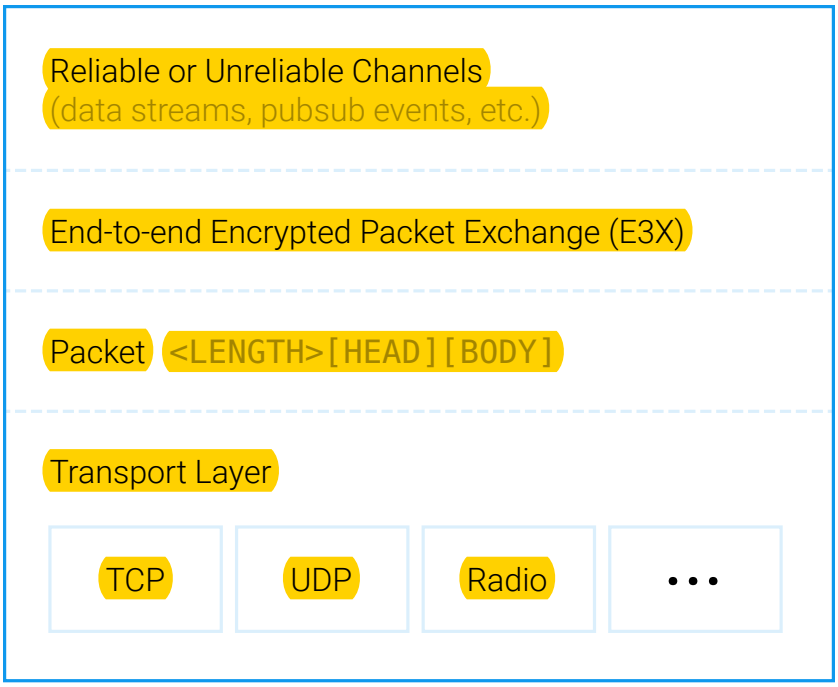
The Filament stack uses telehash for communication among devices. Unlike communication protocols that rely on centralized or federated servers, telehash enables completely distributed, decentralized interaction. Several key foundations make this possible:

- Addresses are not assigned by central authorities, and telehash endpoints do not have accounts at servers. Instead, each endpoint generates its own unique hashname, which is a 32-byte string that corresponds to the SHA-256 hash of one or more public keys. Devices can also have multiple hashnames (generated over different keys) for increased privacy.
- Endpoints can find each other using telehash-native local network discovery or through wide-area methods such as recognized notaries and DNS equivalents (see below).
- There is no unencrypted mode. All messages are end-to-end encrypted all the time using forward secrecy and advanced stream ciphers via the latest industry standards such as JSON Web Encryption (JWE, Jones and Hildebrand 2015, RFC 7516) and JSON Web Signing (JWS, Jones at al. 2015, RFC 7515).
- A message payload is a JSON data structure typically consisting of a binary or JSON header and a binary body; this provides maximal flexibility within a simple encoding scheme.
- Messages can be tunneled over virtually any available transport, including TCP, UDP, TLS, HTTPS, Bluetooth, and mesh networks based on IEEE 802.15.4 radio links.
- Telehash includes built-in cloaking mechanisms that can add random noise to all bytes sent across the wire, which helps to ensure the privacy of activity information and other metadata.
- Messages are passed from one endpoint to another over device-to-device links, which are either direct or mediated by a router (i.e., an endpoint that is willing to forward messages among devices).

Together, these foundations provide private, secure, reliable communications without any dependency on single points of failure such as servers, or even network connectivity outside of the local environment.

The following protocol layer diagram illustrates several of the salient strengths of telehash:

SPADE Protocol Stack



The Filament team has taken telehash a step further using TMesh, a method for secure mesh networking over radio links that provides encoding of communications data into radio parameters, shared management of available spectrum among any number of devices, and establishment of networking relationships among those devices.

Identity

In the Filament stack, identity is tied to the telehash hashname of a device. But how can one device discover other devices and learn more about their capabilities?

On a small scale or on a local mesh - say, a few hundred Filament Taps attached to equipment in a factory - discovery of other devices can occur over WiFi, radio, or even

Bluetooth. This kind of discovery happens organically as devices are provisioned into an installation, because each Tap will naturally establish communication with other nearby Taps using telehash-native local discovery. (Specialized protocols are under development to make this process more organic, and will be described in a future whitepaper.)

Building decentralized, privacy-respecting methods for discovering and introducing devices becomes a challenge when more devices are involved, especially on a wide-area network where physical proximity cannot be leveraged. The Filament team is working on two complementary techniques here:

- Blockname, which provides resolution of addresses through reference to the Bitcoin blockchain instead of the hierarchical DNS tree. To replace the roles played by centralized authorities such as registrars, ICANN, and the 13 root servers in DNS, the Blockname protocol specifies that public or private notaries can vouch for the authenticity of names published into the system. Any organization can run a notary, which gains trust from individual devices and coordinated deployments of devices by operating in a secure, transparent manner consistent with best practices currently employed by certification authorities, such as the methods for verification of physical identity.

- For more ad-hoc interactions (such as when a shipping company's container is placed on a rail company's flatcar), telehash-native local discovery can be used to set up communication; but how can these previously unknown entities bootstrap trust without revealing too much about themselves? Here we apply the age-old custom of incremental disclosure, with a new twist: the seeking device can create a microtransaction that offers currency in return for information about the identity and capabilities of the discovered device.

In both cases, discovery of an address is a necessary but not sufficient condition for enabling contracts and microtransactions, because the capabilities of a device will largely shape the range of possible interactions. Although capabilities will be learned in application-specific ways, it is envisioned that the most useful capabilities will include the data types a device can provide, the actions a device can take (such as routing messages, granting network access, and providing processing power), the protocols and extensions a device supports, and the affiliations that a device has with other devices, larger communities or deployments, notaries, and so on.

Smart Contracts

In conventional service-based applications, permission to interact with a device is typically granted through reference to an access control list (ACL) such as a whitelist of privileged entities. Although more sophisticated policy frameworks exist, in general ACLs are relatively simplistic, allowing or disallowing interaction in an all-or-nothing way. In any case, both ACLs and policy frameworks are instantiated at the service or account level, and thus require communication with a cloud-based API in order for the device to enforce access decisions.

By contrast, the Filament stack leverages several recent innovations to enable smart contracts: self-executing, self-enforcing contracts that are implemented in software (Szabo 1997). These contracts make it possible to specify the particular conditions under which a device will interact with other entities, without reference to a cloud service. Such conditions can include price, the time period during which access is allowed, a per-use charge for defined functionality, attribution for data provided, and other contractual terms that are important to the parties involved. These contracts are specified in a standardized format called JSON Web Token (JWT, Jones at al. 2015, RFC 7519).

Filament technologies enable secure, private microtransactions among autonomous devices.

As a further enhancement, the cryptographic signature and associated headers for a smart contract can be added to a private or public blockchain, thus creating verifiable receipts for contractual obligations. In the Filament stack, such receipts use the Blocklet protocol, which will be the subject of a future whitepaper.

Anatomy of a Smart Contract

HEADER	Hashing Algorithm	
PAYLOAD	***RESERVED***	Issuer, Expiration, Audience, etc.
	PUBLIC	Standard Values (e.g. OpenID Connect)
	PRIVATE	Filament-specific Values
SIGNATURE	Hash of `HEADER` + `PAYLOAD`	

Microtransactions

The ultimate fruit of the foregoing foundations is a method for secure, private microtransactions among autonomous devices. This is needed because the data or service that a device can provide - say, a transient temperature reading or momentary access to network connectivity - is not worth enough to incur the relatively significant transaction costs involved in normal Bitcoin operations.

Blocklet microtransactions solve this problem in two ways. First, currency is exchanged in private side chains that are separate from the public Bitcoin block chain and thus are shielded from Bitcoin transaction costs.
Second, one or both parties to a microtransaction or a series of microtransactions agree to use escrow as a way to lock the value to be exchanged, such that it can be unlocked only after both entities have fulfilled the terms of the contract.

Mesh networks of Filament Taps provide significant savings over cellular and satellite access.

Crucially, this model does not require a centralized service provider such as a Bitcoin-based bank. Although the entities involved might want to engage the services of a third-party auditor for higher-value transactions, such

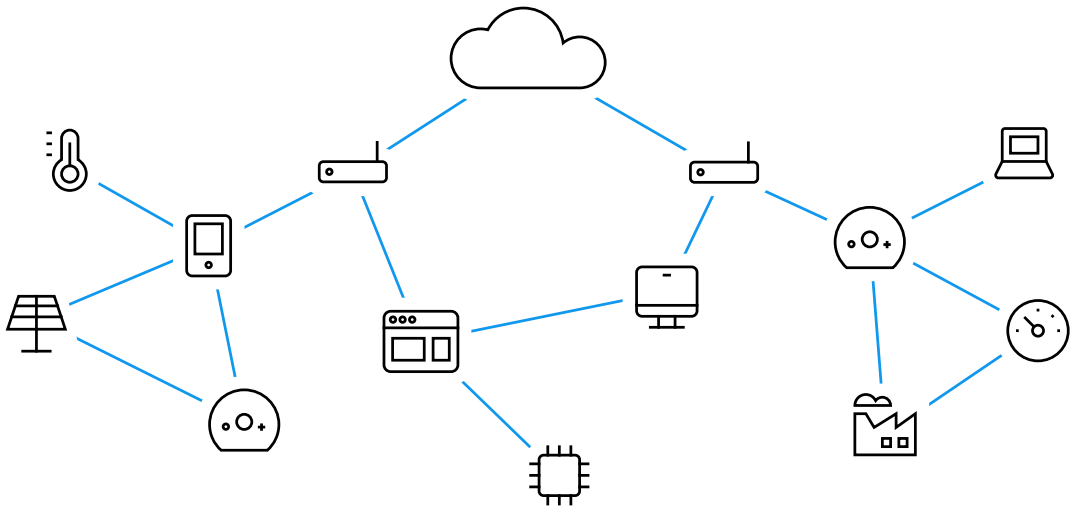
an arrangement is completely voluntary and subject to negotiation. In addition, because unlocking the escrow depends on meeting specified contractual conditions instead of time-based leases, value can be exchanged even if Internet connectivity in unavailable for long periods of time. Finally, as noted above, escrow-based microtransactions can be used to bootstrap discovery and interaction among devices, thus further smoothing the path to completely distributed exchange.

Applications

The Filament team, comprised of industry veterans including the original architects of Jabber/XMPP, has devoted almost ten years and millions of dollars of investment to building the software and hardware foundations for a truly distributed Internet of Things.

Yet we have done so not for the technology itself but for practical applications in industrial scenarios where privacy and security are not just pleasant-sounding buzzwords but mission-critical necessities: energy infrastructure, airports, hospitals, factories, and the like. We have also designed the Filament stack so that it can be used where connectivity is intermittent or simply unavailable: pipelines, power grids, oil and gas fields, and mines are just a few examples of remote locations where Filament Taps fit the bill.

In these scenarios, a typical deployment involves a mesh network of Taps, with more stable nodes acting as gateways to the Internet. Such a deployment leads to significant savings, since the vast majority of Taps do not require expensive cellular or satellite access. In addition, mesh links are based on proximity, enabling endpoints to communicate over long distances through intermediate endpoints that volunteer to route traffic over the network.



Returning to our example of rail transportation, a number of potential applications arise. For instance, manufacturers such as Hitachi have already started to demonstrate the viability of a "train-as-a-service" model (Yoshida 2014), in which the large CAPEX costs of rolling stock and rail infrastructure are converted into more digestible OPEX costs for the customer, who pays only for on-time service. Under this model, it behooves the provider to gather as much information as possible that will help to increase uptime, safely improve delivery times, reduce the risk of derailments, etc. Although end-of-train detectors along with sensors such as hotbox and dragging equipment detectors are standard on rail networks today, inexpensive devices such as the Filament Tap introduce the possibility of monitoring a wider range of data, such as the movement and vibration of individual rail cars (which might indicate, for example, the presence of broken rails or the failure of vehicle running gear).

Naturally, much of the data so gathered will be analyzed in a centralized way using big data methods such as predictive analytics. Yet the gathering itself can be completely distributed across the rail network, with both rolling stock and infrastructure components playing a part. Furthermore, each piece of rolling stock can communicate with others and with the head-of-train device in a locomotive to handle potentially dangerous conditions in real time even if a train is far away from conventional Internet connectivity.

Interestingly, with long-range, sub-GHz radios involved and enough entities empowered with Filament Taps or similar devices, the rail network itself becomes a communications network. This introduces the possibility of selling communication access along the right of way to both fixed buildings (e.g., grain elevators) and things in motion (e.g., intermodal shipping containers). Whereas the cost of cellular or satellite access for some of these entities might be prohibitive, microtransactions for intermittent connectivity might make sense even at the level of each container on a train.

With devices deployed throughout the network, truly autonomous markets for information and contractual interaction become possible, as well. For instance, an intermodal shipping container might be packed at a factory in China, transported via rail to the port of Hong Kong, transferred to a container ship that crosses the Pacific Ocean, unloaded in Long Beach for transport by rail again, and finally delivered to another factory in Dallas for unpacking there. On each leg of the journey, a device associated with the container can engage in secure microtransactions: selling data about its location and cargo, negotiating connectivity to communicate with its owner, signing off on delivery to its final destination, perhaps someday even clearing customs.

Conclusion

The scale of the opportunity for connected exchange is immense (Pureswaran 2015). The science of economics is traditionally divided into macroeconomics - the study of the economic system as a whole - and microeconomics - primarily the study of the millions of firms that interact within that system. Nanoeconomics - a term coined by Kenneth J. Arrow in 1987 to describe interactions among the billions of human beings on our planet - has started to become viable with the widespread deployment of smartphones. Yet the imminent prospect of extending connectivity to trillions of devices opens the possibility of picoeconomics, a thousandfold increase in value exchanged over the nanoeconomics of today.

In parallel, the technological scale of centralized services to mediate such exchange has grown by leaps and bounds. Although the Internet started with just a few nodes each serving thousands or even hundreds of endpoints, today a fortunate few organizations such as Google and Facebook have metastasized beyond megacorporations to become gigacorporations each connecting billions of users. These "gigacorps" have a level of power and control over communication and exchange that is unprecedented in human history.

It remains to be seen whether any organization can scale its technology to become a "teracorp" mediating the interactions of trillions of devices. Even if that is possible, we believe it would be detrimental for human society because of the serious privacy and security implications of centralization at that scale. Furthermore, the inevitable transaction costs involved would overshadow the value of each microtransaction and thus stifle the enormous potential for creating economic value among trillions of devices.

At Filament, we are forging an alternative path: an entirely decentralized network in which autonomous endpoints use smart contracts and private microtransactions to interact and exchange value in completely voluntary and secure ways.

This whitepaper has provided a high-level overview of the technologies needed to make that vision a reality, and future whitepapers will describe them in much greater detail. Although we are still iterating on a number of the necessary building blocks, our design principles are clear and Filament is committed to defining these technologies in a transparent way to ensure technical excellence, ethical design, community involvement, and continuous improvement in customer deployments. Contact us via hello@filament.com to be kept informed about the latest developments.

References

Cooper, A., H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith. 2013. RFC 6973: Privacy Considerations for Internet Protocols. https://www.rfc-editor.org/rfc/rfc6973.txt

Dierks, T. and E. Rescorla. 2008. RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2. https://www.rfc-editor.org/rfc/rfc5246.txt

Jones, M., J. Bradley, and N. Sakimura. 2015. RFC 7515: JSON Web Signature (JWS). https://www.rfc-editor.org/rfc/rfc7515.txt

Jones, M. and J. Hildebrand. 2015. RFC 7516: JSON Web Encryption (JWE). https://www.rfc-editor.org/rfc/rfc7516.txt

Jones, M., J. Bradley, and N. Sakimura. 2015. RFC 7519: JSON Web Token (JWT). https://www.rfc-editor.org/rfc/rfc7519.txt

Pureswaran, V. 2015. "Device Democracy: Saving the future of the Internet of Things." http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

Saint-Andre, P. 2015. RFC 7622: Extensible Messaging and Presence Protocol (XMPP): Address Format. https://www.rfc-editor.org/rfc/rfc7622.txt

Szabo, N. 1997. "Formalizing and Securing Relationships on Public Networks." http://firstmonday.org/ojs/index.php/fm/article/view/548/469

Yoshida, H. 2014. "Internet of Things and Train as a Service." https://community.hds.com/community/innovation-center/hus-place/blog/2014/11/07/internet-of-things-and-train-as-a-service