Particle

PARTICLE SECURITY ARCHITECTURE AND PRIVACY OVERVIEW

Bringing the physical world online safely and securely.

PARTICLE SECURITY ARCHITECTURE AND PRIVACY OVERVIEW

When you choose to build on Particle, you're inviting us into your products and onto your customer's networks. As a result, we recognize the level of trust you're placing in us to always do the right thing when it comes to data security and privacy. We take this responsibility extremely seriously.

By now, the vast majority of us have been personally impacted by a data security breach, and as it turns out, many organizations that have suffered any type of compromise "take the security of your information extremely seriously". Given this, we could all be forgiven for being a little skeptical about such claims. In this day and age, when we consider the secure handling of information, trust, very rightly, has to be earned.

The purpose of this document is to provide a starting point, as we, at Particle, begin the journey of earning your trust. It will take you on a tour of Particle's security, privacy, and trust practices from the top down. Beginning with our organizational level practices and principles that guide our design decisions that flow into our services, software, and hardware. But it is just that; a starting point. The majority of trust comes later. It will be built as we work together, and as you interact with the Particle team.

After all, when you partner with Particle, you're getting more than just a hardware component or a piece of software. You're expanding your team to include the security, reliability, and engineering expertise of Particle. We don't doubt that as you engage with us, you'll find yourself exposed to a group of people who are just as passionate about keeping your data secure as you are.

Particle the Company

Our employees are globally dispersed and highly diverse, but they all have one thing in common. Everyone at Particle, regardless of tenure, location, or position, undergoes an annual security and privacy training session to make sure they are up to speed on how best to operate securely. Critically, everyone knows where to go to ask questions and get advice on security issues, and how to raise the alarm in the event of a suspected security incident.

Particle's security principles

The security program at Particle is founded on four key principles.

1. **Security in everything we do** – Particle aspires to ensure that security is a primary consideration in any activity performed during our operations. Whether that is working with customer information, building a new feature in our software or hardware products, or merely using a computer to research something online.
2. **Security is for everyone** – The policies within the Particle security program apply to everyone who has been provided access to Particle computing assets, including, but not limited to, employees, independent contractors, business partners, and vendors.
3. **Security applies everywhere** – The policies within the security program apply to Particle computing assets and data, no matter the form factor or physical location of the asset.
4. **We act based on globally recognized standards and guidelines** – The Particle security program is based on the International Organization for Standardization's ISO 27001:2013 standard, widely regarded as the gold standard for organizational security.

A dedicated security team

Particle maintains a dedicated security team to support both customers and employees in the operation of our security and privacy program. The team contains professionals with significant experience in secure development, security operations, and incident response. Some examples security industry certifications maintained by team members include:

- Certified Information Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- HealthCare Information Security and Privacy Practitioner (HCISPP)

- Certified Ethical Hacker (CEH)
- Certified Computer Hacking Forensic Investigator (CHFI)
- AccessData Certified Forensic Examiner (ACE)
- Certified Cyber Forensics Professional-US (CCFP-US)
- Security+ Certification

The core responsibilities of the Particle security team include:

- **Security operations** - monitoring the Particle Device Cloud and corporate networks for indicators of malicious activity, and responding accordingly.
- **Application security** - working with engineering teams to build security features into the Particle platform, and ensure vulnerabilities are effectively managed.
- **Compliance and privacy operations** - ensuring Particle's continued operation per the requirements laid out in regulatory standards and contractual agreements. This also includes managing third-party audits to ensure continued compliance.
- **Identity and access management** - enforcing the principle of least privilege in regards to access to data and systems.
- **Risk management** - identifying, tracking and treating enterprise risks to ensure the continued prosperity of Particle and our customers.

Technical security

All Particle employees are issued with company laptops that run centrally managed, enterprise-grade antivirus and data-loss prevention software. Our laptops also run asset management tools that allow the Particle security team to ensure they are compliant with our technical security standards, for example, leveraging full disk encryption and strong passwords.

Particle employee accounts are protected by two-factor authentication, and robust onboarding and offboarding processes that ensure the timely removal of access for employees should they leave the company.

Security beyond the office

With a remote and flexible workforce, the traditional 'office network' has less of a bearing on security than it once did (although, don't worry, we still monitor these with technologies such as intrusion detection systems). To this end, Particle's security team is focused on empowering employees to maintain secure networks at home. One of the ways we achieve this is by offering free home antivirus software for up to 10 devices, as an employee benefit, available to all employees.

Responsible disclosure

As an organization with a long history of transparency, and working closely with our developer community, it should be no surprise that Particle extends the same philosophy to our relationship with security researchers acting in good faith. Particle actively operates a responsible disclosure program to ensure that researchers who report discovered vulnerabilities in our products are protected and also compensated for their work where applicable. This program has directly resulted in security improvements within Particle products and services.

Privacy at Particle

It's an exciting time, as consumers are being afforded more rights in respect to the privacy of their personally identifiable information. New and evolving legislation, such as the General Data Protection Regulation (GDPR), which went into effect in the European Union in 2018, and the California Consumer Protection Act (CCPA) that went into effect in 2020, provides residents of those jurisdictions a set of exercisable rights regarding their data. The two examples are likely the first of many, as legislative processes catch up with the role of technology in our connected lives.

Privacy Shield
Framework

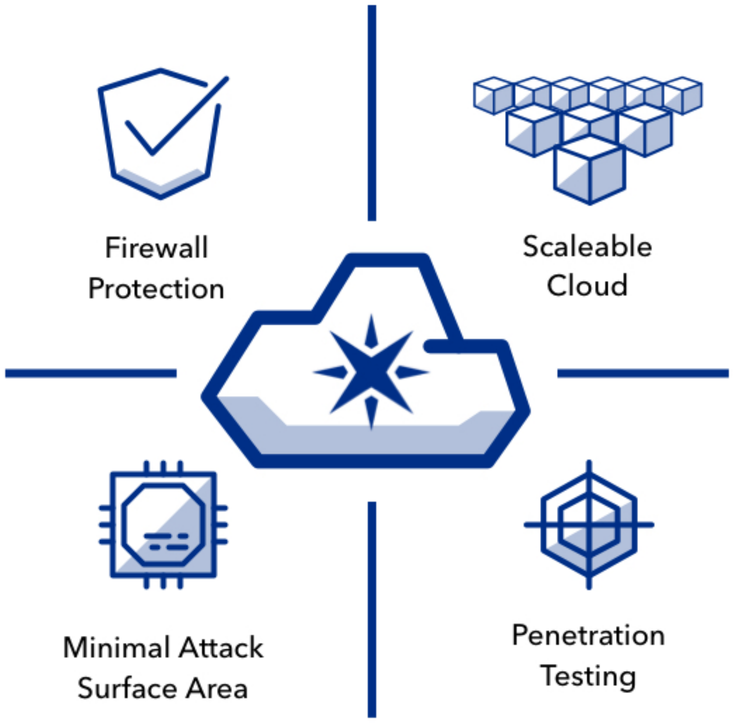
EU-US and Swiss-US Privacy Shield Compliance

To further solidify our commitment to privacy, Particle is an active member of the EU-US and Swiss-US privacy shield framework. As a company based in the United States, with customers and employees based in the EU, it is tremendously important to us that we have processes in place to protect the personal information of EU residents. Our participation in the Privacy Shield provides this level of assurance, to both our direct and indirect customers.

Privacy for all

Particle's privacy practices are designed to extend to all users of our platform, regardless of citizenship or physical location. We believe that everyone should have the same rights in regards to how their information is handled. Our processes can be applied to any person who is leveraging our platform, directly or indirectly.

Particle Device Cloud



All Particle devices communicate through the Device Cloud. This setup ensures a consistent operation environment and allows devices to operate solely in a "reverse connecting" mode (i.e. Particle devices connect back to the Device Cloud, rather than requiring firewalls changes to allow inbound connectivity. This setup eliminates the need for open ports, hardcoded default passwords, and other active-side attack surface elements that are frequently associated with IoT devices.

The Device Cloud affords you with a single view into your entire fleet of devices and is built to scale with your product. Data published by Particle devices flows into the Device Cloud, and out through integrations to your environment.

By default, no customer data beyond device metadata is persisted in the Device Cloud. The Device Cloud has been built from the ground up with security in mind. It's designed to take advantage of the ingrained secure-by-default features provided by industry-leading, infrastructure as a service (IaaS) providers (who meet the needs of various security standards and compliance frameworks, including ISO27001 and SOC II), and free of legacy components. This gives Particle's security and engineering teams perhaps the most critical ingredient in any effective security program visibility.

To protect something, you first must know that it is there. This seems like an extremely simple concept, and it is, but ask anyone responsible for security at an organization if they truly believe they have complete visibility; you might get more than a few hesitant answers. That's why we've made visibility such a key focus at Particle. It's the cornerstone of our Device Cloud security program. We can confidently say that we have visibility into every component in the Device Cloud environment.

Visibility and auditability

If it moves in our environment, we make sure we know about it. If it involves your data, we make sure you know too. We do this through an open event logging framework that allows you and your team to get an instant overview of how a given device is operating.

Transport-layer cryptography

All communications between Particle devices and the Device Cloud are encrypted, with no opportunity for cleartext communication to occur. Every device ships with a unique device-specific RSA or Elliptic Curve key-pair, and has a pinned Cloud public key.

Device keys are generated during manufacturing and the public key is pinned in the cloud. Strong unique keys and bidirectional pinning prevent rogue actors from impersonating one of your devices or intercepting your data using a man-in-the-middle attack. Active measures have been deployed to detect potential cloned devices and alert the security team.

Our TCP service, leveraged by devices connecting over Wi-Fi, uses an RSA handshake to establish a session key for a fast rotating AES session. Each message is encrypted and is checked via a message ID for replay attacks or out-of-order messages. Any anomaly causes it to immediately end.

Our devices include hardware random number generators compliant with FIPS 140-2 and the RSA/AES cloud handshake includes a cryptographically random nonce, to ensure there is sufficient randomness on these low-power devices.

Our UDP service, leveraged by devices connecting over cellular, uses DTLS, a version of TLS designed for low-bandwidth and lossy UDP packets. TLS is the standard for secure browser traffic worldwide. Particle leverages the open source mbed TLS library supported by ARM and used by other security conscious companies such as OpenVPN, nginx, and Linksys. We use 256 bit ECC keys for our DTLS service, roughly equivalent to a 3072-bit RSA key.

We believe that strong cryptography should be based on established best practices and algorithms, and that the use of these standards should be transparent. If a secure communications system can't withstand public scrutiny, then it's not sufficiently secure. This is why we've open-sourced our encryption protocols and techniques. All the device communication source code is available via Particle’s Github organization.

Role-based access control (RBAC)

Particle supports varying levels of access to your device fleet through the Device Cloud, allowing you the ability to maintain your own ‘least privilege’ stance (i.e. giving people the least amount of access required to perform their duties) when working with the Particle platform.

Transport-layer cryptography

All communications between Particle devices and the Device Cloud are encrypted, with no opportunity for cleartext communication to occur. Every device ships with a unique device-specific RSA or Elliptic Curve key-pair, and has a pinned Cloud public key.

Device keys are generated during manufacturing and the public key is pinned in the cloud. Strong unique keys and bidirectional pinning prevent rogue actors from impersonating one of your devices or intercepting your data using a man-in-the-middle attack. Active measures have been deployed to detect potential cloned devices and alert the security team.

Our TCP service, leveraged by devices connecting over Wi-Fi, uses an RSA handshake to establish a session key for a fast rotating AES session. Each message is encrypted and is checked via a message ID for replay attacks or out-of-order messages. Any anomaly causes it to immediately end.

Our devices include hardware random number generators compliant with FIPS 140-2 and the RSA/AES cloud handshake includes a cryptographically random nonce, to ensure there is sufficient randomness on these low-power devices.

Our UDP service, leveraged by devices connecting over cellular, uses DTLS, a version of TLS designed for low-bandwidth and lossy UDP packets. TLS is the standard for secure browser traffic worldwide. Particle leverages the open source mbed TLS library supported by ARM and used by other security conscious companies such as OpenVPN, nginx, and Linksys. We use 256 bit ECC keys for our DTLS service, roughly equivalent to a 3072-bit RSA key.

We believe that strong cryptography should be based on established best practices and algorithms, and that the use of these standards should be transparent. If a secure communications system can't withstand public scrutiny, then it's not sufficiently secure. This is why we've open-sourced our encryption protocols and techniques. All the device communication source code is available via Particle’s Github organization.

Role-based access control (RBAC)

Particle supports varying levels of access to your device fleet through the Device Cloud, allowing you the ability to maintain your own ‘least privilege’ stance (i.e. giving people the least amount of access required to perform their duties) when working with the Particle platform.

Multi-factor authentication

Particle Device Cloud accounts support the use of multifactor authentication (MFA), using your preferred MFA application.

Geolocation data

When leveraging location services provided by Particle, GPS coordinates will be persisted by Particle on a rolling retention basis. Given the sensitive nature of GPS data and the fact that the data is one of the few elements we retain, dedicated infrastructure has been created to ensure the data is segregated from the rest of the Device Cloud platform. Access to geolocation information is strictly controlled, and limited to only those Particle employees with a need to access it.

Security operations and the device cloud

When you choose Particle, our security team becomes your security team. We actively monitor the Device Cloud for security events that could indicate an issue with your devices. Through the use of a custom-built security incident and event management suite (SIEM) created by the security team, Particle specific security events are generated internally that can be relayed to customers as required.

Some examples of security events we actively monitor for in the Device Cloud include:

- Devices connecting from potentially hostile networks/environments (based on threat intelligence feeds).
- Accounts that are at risk of credential stuffing attacks due to password reuse.
- Potentially cloned devices.
- Scans and probes against the Device Cloud.
- Attempts to subvert rate limits to cause denial of service, or other unexpected behaviors.

Intrusion detection

Particle’s Device Cloud environment is protected by a continually-updated intrusion detection system (IDS) that is actively monitored by the Particle security team via the SIEM tool.

Microservices and containers

Device Cloud infrastructure operates as microservices, with zero monolithic components. Container images are regularly recycled, and deployments are designed to scale automatically with load, resulting in a stable and secure experience.

Infrastructure management

Particle's engineering teams leverage a VPN protected by multifactor authentication to gain access to the Device Cloud to perform maintenance and monitoring. Activity on the VPN is fully audited and access is only provisioned to those who need it.

Separate staging and production environments

Particle maintains completely separate staging and production environments to ensure that there is no cross-contamination of customer data during development and test work.

Vulnerability management

Particle's vulnerability management program leverages two distinct methods for identifying software vulnerabilities. Static scanning is performed on code that makes its way into our products. to ensure that vulnerable dependencies and libraries are patched as soon as possible.

Dynamic vulnerability scans within the Device Cloud also occur to validate that all software is as secure as possible.

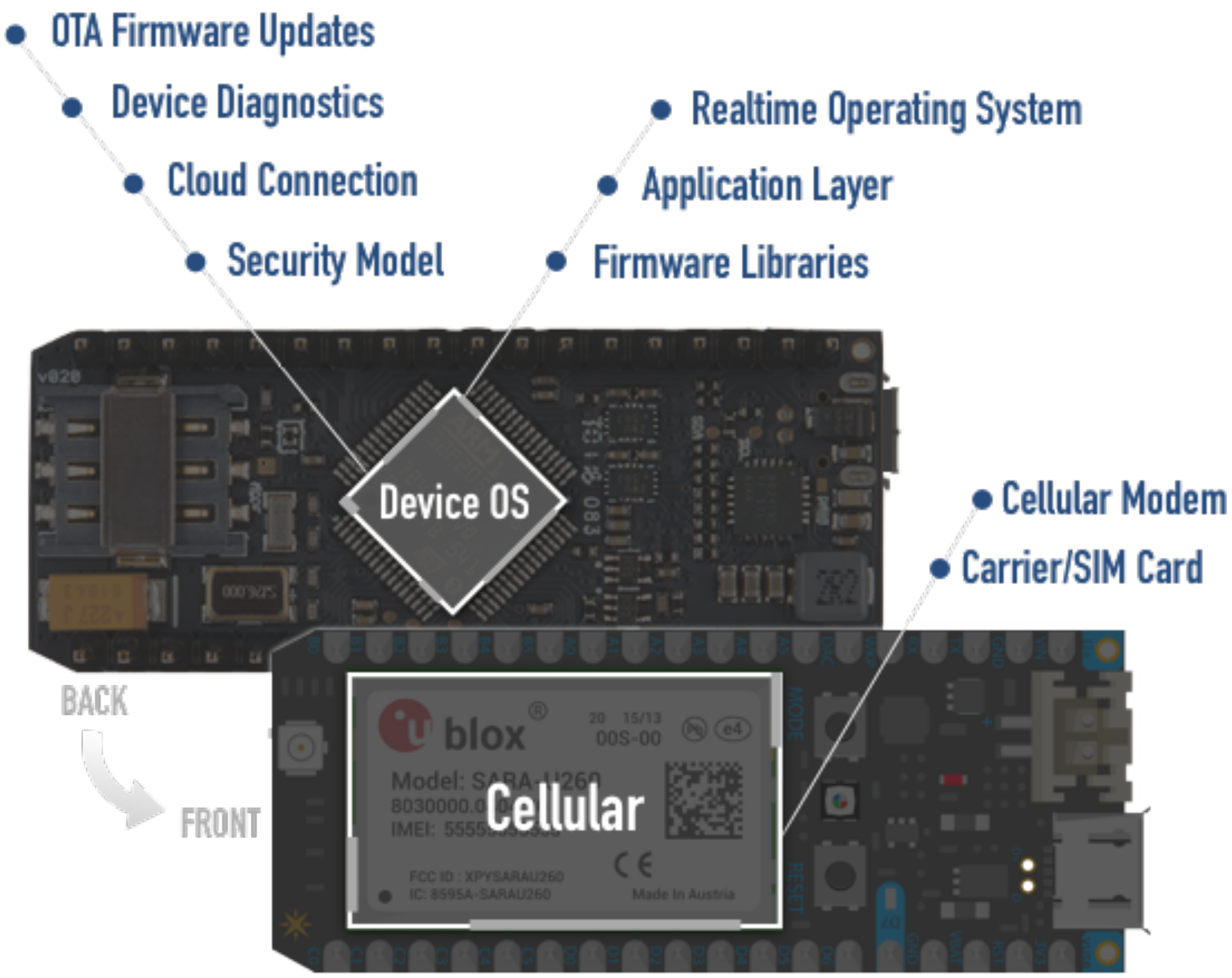
Particle Device OS

Particle has developed the Particle Device OS: a powerful, open-source, operating system that runs on all Particle devices.

Device OS abstracts the complex integration between microcontrollers, modems, peripherals, verified libraries, and your application firmware needed to get a physical device working seamlessly and securely for your product. Device OS is constantly maintained and released on a regular cadence and represents ongoing improvements, learning, and robust performance for devices distributed to a community of over 140,000 developers across 8 years. Device OS development has taken over 115,000 hours (55 EP) and has nearly a dozen engineers executing regular maintenance and extending functionality.

The Device OS is subject to the same rigorous application security requirements and processes as the Particle Device Cloud, and given that it is open source, is frequently inspected for security issues.

Other Device OS responsibilities, include:



Secure cloud communications

Device OS manages a secure session with the Particle Device Cloud (pinned keys, RSA/AES, DTLS).

Hardware abstraction layer (HAL)

A consistent and well maintained interface to underlying hardware and peripherals for firmware development.

Feature rich firmware API

Our firmware API wraps powerful, common functionality for rapid development.

Real-time operating system (RTOS)

Our RTOS enables your product to support precision demands and responsiveness in the field.

Over the air updates

Every connected device requires a mechanism to update firmware reliably. Our OTA Firmware offering allows you to do just that and is proven in areas with poor connectivity. Performing an OTA update should not need to be done with crossed fingers though; at all times you remain in control of your devices, and your patching program. You can pin your firmware against a known long-term-release of system firmware for added stability, or allow the automatic upgrading system to keep your products up to date as you deploy new releases.

Low power modes

Leveraging low power modes to lengthen battery life of the unit while still being connected to the cellular network.

Resilient communication

Device OS automatically retries dropped messages as needed, and seamlessly roams between servers or cellular infrastructure in the field, while also using minimal data.

Particle Hardware

All the services and components we've discussed so far sit atop our hardware to deliver a secure IoT experience. Maintaining a secure, authenticated connection to the Particle Device Cloud gives you confidence to deploy firmware and issue commands to your devices. Some of the elements that make Particle hardware secure include:

- **An embedded microcontroller with real-time operating system (RTOS)** – decreases the potential for physical attacks.
- **Secure ports** – no incoming ports are open for port scanners to discover, or other or active side attacks.
- **Encrypted connections** – radio connections encrypted with WPA2 or standard cellular radio protocols.
- **Secure device protocols** – adds future proofing and end-to-end encryption to the cloud.

The device is also protected against failures during the Over-The-Air (OTA) firmware update process. Each firmware module includes a verifiable hash, and metadata to ensure the code is appropriate for that platform and product. If corrupted firmware is sent to a device, or a mismatched firmware for that product, the device will safely fail-back to the last known good firmware stored locally in flash.

Product creators can also pin a known version of firmware for their products, which the Device Cloud will enforce, to help ensure your customers are getting the best experience. The firmware is also split into modules, so the speed of the update is as fast and as low risk as possible, minimizing any interruptions during an update.

Additionally, regardless of whether devices connect via Wi-Fi or Cellular, or other radio protocols, the network authentication credentials are never transmitted to the Device Cloud, and are only stored locally or on a SIM card.

A trusted partner, from day one and beyond

Particle serves a number of product creators and enterprises across different industries. Whether you're building your first prototype, or leveraging Particle to deploy your one-thousandth unit, you can rest assured that you're being backed by the people, processes, and technologies you need to do so securely.

Everything that we observe and learn in the field is worked back into our products and services on an ongoing basis. Security is a journey, not a destination, and we hope you'll join us along the way.

Further reading

Particle maintains a wide set of documentation and other materials relevant to our security program that are available by request, and where applicable, under a non-disclosure agreement (NDA). If you would like to review any of the following, please reach out to your account executive:

- Particle security policies and procedures
- Latest vulnerability scan results
- GDPR/CCPA third party audit report
- Security architecture diagrams
- Latest penetration test report
- Rules of engagement for customer penetration testing

We also welcome any further questions on security or privacy practices, please reach out via your account executive, who will route your question appropriately.