SECURITY

How we make sure sensor data is private and secure

Introduction

At Disruptive Technologies (DT), we have prioritized security and privacy throughout the design and development of our sensing solution, including chip design, sensor design, radio protocol design, cloud services, and APIs.

Every layer is secure, from the individual sensors to the applications processing the data. Measurement and sensor identity data are encrypted within the sensors themselves. The data stays encrypted through radio transmission and cellular or Ethernet forwarding over the Internet until it reaches the secure DT Cloud. The data is then passed to customer applications via encrypted protocols. Access control mechanisms in the DT Cloud provide controlled delivery of sensor data to designated processing systems.

With a fully secured system, our customers can focus on using data to meet their business goals and not worry about unintentional data access.

SecureDataShot: Innovating IoT Security

Unlike IoT technology that connects devices and data through a gateway, the DT solution uses Cloud Connectors that relay data to the cloud without storing it to remove typical security weak points in the IoT architecture and simplify implementation and maintenance. We call this revolutionary end-to-end secure solution SecureDataShot™ (visualized in Figure 1).

This architecture virtually eliminates potential manipulator-in-the-middle attacks that exploit gaps in gateway security architecture. Pairing sensors directly with users is easier and faster than pairing sensors to a gateway.

In our architecture, multiple Cloud Connectors allow for roaming to eliminate bottlenecks. Initial installation and extensions to an existing installation are significantly faster using the Disruptive Technologies architecture than a gateway-based system.

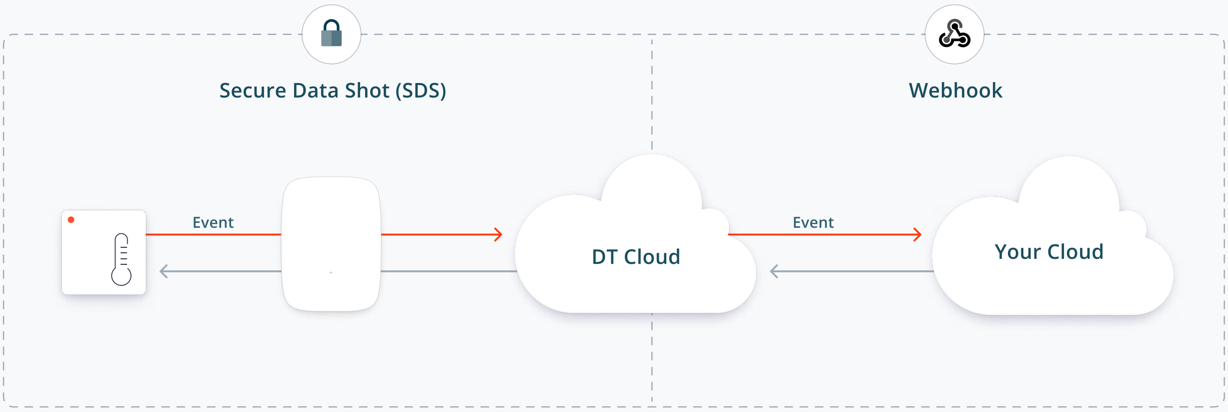
Crypto Key Installation & Storage

Each sensor is assigned a unique 256-bit asymmetric encryption key when manufactured. Key generation is managed by a tamper-proof FIPS 140-2 Level 3 certified hardware security module. The public part of the asymmetric encryption keys is exchanged with DT’s cloud via encrypted channels. The private part never leaves the storage in the sensor.

Encryption keys are generated and installed in a secure production facility with limited and audited access control. When the public keys are securely exchanged, the sensor and the cloud authenticate each other and establish a tamper-proof, end-to-end encrypted communication channel using modern cryptographic standards. DT holds patents on how to do this in a secure and energy efficient way on a resource constrained device.

Cloud Connectors have Transport Layer Security (TLS) certificates to establish secure, mutually authenticated connections and guard against manipulator-in-the-middle attacks targeting the DT Cloud.

In the DT Cloud, cryptographic keys are stored in separate components, locked down, and unavailable to the rest of the system except when they are used to establish ephemeral session keys. For protection against loss, encrypted backups of device keys are stored in multiple secure locations.



Wireless Sensors

Wireless sensors instantly connects and send data to the cloud via SecureDataShot™

Cloud Connectors

Cloud Connectors automatically connect and relay data to the cloud service.

Cloud Service

No servers, databases, or on-prem clients to manage - simply just install sensors and integrate the data into your own service.

Figure 1. SecureDataShot™ removes typical "manipulator-in-the-middle" security weak points using mutually authenticated end-to-end encryption.

Cloud Platform & System Monitoring

DT Cloud components run in Google Cloud and are managed by one of the most advanced security organizations in the world, with top-level security controls. We follow security best practices for each of the components in use. The DT Cloud also uses Google Infrastructure services and relies on their security to protect against attacks.

All system components are instrumented and monitored 24 hours daily, seven days a week. Anomalies outside operational parameters trigger alarms and automatically notify our response team to initiate appropriate investigations and, if necessary, escalation procedures. Updates are rolled out to Cloud Connectors and sensors as part of the DT subscription service.

End-to-End Encryption

The illustration in Figure 2 highlights the following characteristics of the system:

- Encryption keys allow sensors to communicate securely with the Cloud, regardless of how communication packages are routed through different Cloud Connectors or how they are connected to the Internet.
- The same package may be routed through multiple Cloud Connectors to the cloud, but only one will forward a reply package. The Cloud manages which Cloud Connector will respond to which sensor based on signal strength and communication history.
- Replies from the Cloud back to the sensor, which may be simple ACK packages or more complex configuration updates, are also encrypted from the Cloud and cannot be decrypted until they are on the sensor itself.
- The Cloud holds unique session encryption keys for each sensor.
- Each sensor holds its own keys, and the session key is generated for communicating with the Cloud.
- The communication channels from each Cloud Connector, through which some additional metadata, such as offline/online status and cellular signal strength, are established using mutually authenticated, encrypted TLS channels. These channels are established via pre-installed security certificates on each Cloud Connector.

Third Party Verification

We have completed multiple independent security reviews conducted by Radically Open Security, a security firm recognized for its transparency; Praetorian, a cybersecurity solutions company; UL, a global safety consulting and certification company; and security expert Lars Lydersen.

It is the responsibility of Disruptive Technologies to audit any changes to its products, systems, and services continuously, with a maximum time between audits of 18 months.

Data Ownership

The end-user owns the data processed through our solution, and the DT Cloud connects data from connected sensors.

The data entered into the system by a user via Studio or our APIs is protected by DT as the user's property using the same security mechanisms used to protect sensor data.

Data Access and Restrictions

By default, our developers do not have access to production data. The number of DT personnel with system access to production data is minimal. Access to production data generates an audit log, and a customer's data protection policy specifies rules for such access.

Customers can access sensor data via the Studio web application, Data Connectors (webhooks), and the use of our API. Data Connectors are controlled through the same access mechanisms as other device information and can only be configured by personnel with sufficient permission levels. Data required by DT to analyze sensor performance, energy consumption, and lifetime estimates are managed according to contract terms for such use.

Data Connectors & Streaming API Methods

Data Connectors push data to endpoints configured by the customer. Only encrypted channels are accepted. Customers can provide a secret to each Data Connector, which will be used to cryptographically sign each event and the data forwarded to the Data Connector. By verifying the signature on the receiving side, customers may confirm that no unauthorized third party can send or forge data into their reception point undetected.

For some applications, the API allows setting up streaming connections that listen to a subset of sensors in a project. All API access is authorized through access rights granted to service accounts.

The API user must authenticate the API access through valid service account credentials, and the service account access rights will limit what the API access will allow. Service accounts and their access rights are controlled by customers, either through Studio or programmatically through the API.

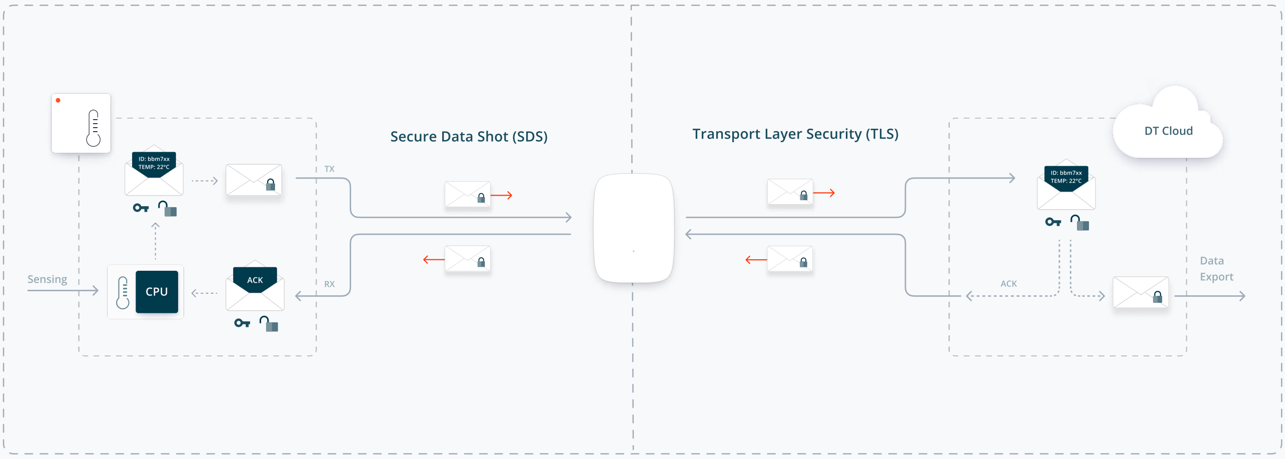


Figure 2. Overview of the how encrypted data is sent between sensors and the DT Cloud.

Privacy

The EU General Data Protection Regulation (GDPR) is an important legislation intended to strengthen and unify a consistent personal data protection framework across Europe.

Personal data is any information relating to an individual that can be directly or indirectly identified. The GDPR distinguishes between companies that act as data controllers and data processors. The data controller determines the purposes and means of processing personal data, while the data processor processes data on behalf of the data controller.

Customers will typically act as data controllers for any personal data they handle concerning their use of DT services, while Disruptive Technologies is a data processor. As data controllers, customers are required to assess whether their data processor is meeting the requirements of the GDPR.

DT’s corporate GDPR compliance includes implementing technical and organizational measures to ensure security appropriate to the risk, such as Data Processing Agreements (DPA) developed for customers and suppliers.

- GDPR owner appointed (contactable via e-mail at compliance@disruptivetechnologies.com)

- Personal Impact Assessments (PIA). Our review method is based on recommendations by European advisory bodies on data protection and privacy and addresses questions related to device and system security, access control, and data management. As part of this review, we have evaluated our ability to support our customers in performing their duties as data controllers.

Data Storage Locations

All sensor and Cloud Connector data are stored in Google data centers in the European Union. The Google Cloud Platform complies with applicable EU privacy and data protection regulations.

Conclusion

At Disruptive Technologies, security and privacy are a priority, not an afterthought. We have ensured security throughout our product design and development process by building security controls and rigorously testing them. Our customers can trust that data captured by our sensors remains private and secure.