Matter is the foundation for connected things, an industry-unifying standard to deliver reliable, seamless and secure connectivity.

### Matter Security Principles

The concern of cyberattacks can create hesitation in the minds of consumers, limiting adoption. With this in mind, Matter was created with security and privacy as key design tenets and provides a baseline for building secure IoT devices.

#### Comprehensive
- Layered approach with authentication and attestation for commissioning
- Every message protected
- Secure over-the-air firmware updates

#### Strong
- Single strong cryptographic suite based on well-established standards
- Passcodes and certificates used to setup secure sessions
- Device attestation to ensure authenticity

#### Easy
- Designed to make smart devices easier to implement and use

#### Resilient
- Designed to protect, detect and recover
- Distributed Compliance Ledger to enhance resiliency and scale

#### Agile
- Crypto-flexibility to address new developments and threats

### Platform Security

Matter provides guidance to device manufacturers to select the appropriate platform security related to the risk and threat analysis of the use cases associated with their devices.
Matter Privacy Principles

Data privacy aims to protect consumers whose personal information is consumed and transacted. Matter embeds data privacy principles for all interactions between devices and software agents that handle personal information. For complete protection, additional support from the environment and infrastructure that Matter devices operate in is needed.

Confidentiality & Integrity
Matter uses the highest possible level of civilian cryptographic standards for network communications to ensure that unauthorized entities cannot easily access or tamper with data communicated between Matter devices.

Proof of identity
Required for Matter devices with cryptographic certificates so data is shared only between known Matter entities.

Open standard
Enables anyone to inspect the template for Matter interactions between legitimate Matter nodes.

Minimizing data
Data shared within Matter interactions is minimized, thereby reducing the potential for inadvertent leakage of information.

Defined purpose
Data shared between Matter nodes is strictly for a defined purpose, namely, for the specific operations of devices as required by the Matter protocol.

Privacy preserving mechanisms
Encryption to ensure that messages or identities of communicating parties are not in cleartext on the network.

Foundation for connected things

- Simplicity
  Easy to purchase and use
- Interoperability
  Devices from multiple brands work natively together
- Reliability
  Consistent and responsive local connectivity
- Security
  Robust and streamlined for developers and users

Learn more at www.buildwithmatter.com. Find out how to become a member at csa-iot.org today.