Securing the printer as a secure IoT device

- The Sigma printer TPM2 is used to store the Crypto keys and it is used as a cryptographic engine for encrypting/decrypting crypto keys during TLS operations in-system.
- Secure Boot: With the Secure Boot, the firmware shall ensure that only authentic firmware images are used to boot the printer by validating their digital signatures.

Protecting data

IIDaaS provides the following to help secure customer data through the lifecycle:

- Data Creation: When data is created by the user in a browser environment, we support technologies like content security policy to leverage features of modern browsers to enhance data protection.
- Data in Transit: We support industry standard protocols such as TLS. IIDaaS provides features to encrypt the channels through which data flows between users, services, databases, authentication systems, and more, reducing the possibilities of man-in-the-middle attacks.
- Data at Rest: We use strong crypto algorithms and keys to protect data.
- Printer to Message Broker: In IIDaaS printer to message broker, communications are encrypted using TLS to provide confidentiality. Printer to Broker authentications are enforced by JSON Web Token (JWT) authentication mechanism using strong

Protecting the application that processes the data

IIDaaS provides the following application

ENTRUST