LAUDA.LIVE IOT PLATFORM – SECURITY INFORMATION

The LAUDA.LIVE services provide a new set of features in the field of temperature control. Functionalities from proactive support to online process analysis are possible thanks to the IT infrastructure set up by the LAUDA experts. Making use of the most trusted tools, the LAUDA.LIVE ensures security at every level.

This document presents a clear view of the information flow and the security measures prepared for the Internet of Things (IoT) solution. There a brief overview about the following four points is provided:

- Cloud Hosting
- Data Gathering and customer control about data permissions
- Data Storage
- LAUDA.LIVE website and user access

CLOUD HOSTING: MICROSOFT AZURE

Using the Microsoft Azure infrastructure to set up the application, we can rely on an experienced partner to host state of the art encryption mechanisms that guarantee that only the LAUDA Service Team can access your data. With the flexibility the Cloud offers, it allows us to scale along with the demand always ensuring a fast response.

Within our Azure account, several managed resources (Virtual machine, SaaS, App services) handle different digital services that take part in the LAUDA.LIVE solution. In this way one service is isolated from the others, in such a way that the failure of a service doesn't compromise the rest. In addition, essential services for user experience will be duplicated.

All the services are encapsulated and external communications will only be allowed to the service hosting the website, the IoT Hub (for gateway) and Jitterbit (provide information to the IT solution Salesforce™). For LAUDA device and gateway configuration, access is secured by asymmetric cryptography and shared access signature tokens.

We are following the Microsoft Azure architecture and security recommendations and are using whenever it is possible Microsoft Azure services.

DATA GATHERING: DEVICES AND GATEWAYS

Some LAUDA devices can directly interface with the Cloud. For some devices, a gateway is mandatory in the sense that Cloud connectivity is not built into the devices directly. These devices handle the communication with the Azure IoT Hub, which will set the course for further processing and storage.

Device security features include:

- LAUDA.LIVE device communication needs to be enabled by the customer in the device menu (for detailed information see LAUDA device manual)
    - Customer controls additional permissions for device data (read only or read/write)
- LAUDA devices do not accept unsolicited network connections. They establish all connections and routes in an outbound-only fashion. Once a connection between the device and Azure IoT Hub is securely established, messaging from the cloud to the device and device to the cloud can be sent transparently
- LAUDA device registration and authentication is done by the Microsoft Device Provisioning Service (DPS) based on X.509 certificates, which creates a unique identity key for each device.
- The unique identity key is the basis of a token used in all communication between the device and the Azure IoT Hub.
- System-level authorization and authentication use per-device identities, making access credentials and permissions near-instantly revocable

The main method to secure and verify our machines' software is through LAUDA Public Key Infrastructure (PKI). According to RFC 3647 (Internet X.509 Public Key Infrastructure), LAUDA certifies each device and its software. This system for identification of each device and the LAUDA member who certified them, as well as where their credentials come from, obtaining complete traceability.

Additionally, when the machine tries to register to the LAUDA.LIVE it will only be able to do so if the Azure Device Provisioning Service can identify a device valid certificate. Therefore, the PKI doesn't just prevent that non-certified software is used, but also avoids that non-trustworthy devices can upload information.

Each connection is secured using state-of-the-art Transport Layer Security (TLS), an encryption algorithm specialized for securing connections over the internet.

DATA STORAGE: SQL AND ELASTICSEARCH

The device information gathered is stored in two different Azure managed databases, depending on the nature of the stored data:

- The telemetry information and analysis generated are stored in the fast and flexible database Elasticsearch. This database will be able to host as much data as requested with better performance than structured databases for the high amount of data that is gathered.
- The user information and alarms are stored in a SQL database in a separated Azure managed service. This database stores sensitive information (log in information and Multi Factor Authentication (MFA)) that is managed in a more careful way.

Only whitelisted IPs and internal Azure services can communicate with the database. From the user's perspective only the WildFly webserver hosting the website can access these databases to provide the different dashboards with the device and user information, as well as to verify log ins. In addition, all services are part of subnets and Azure security groups to ensure restricted access for services.

LAUDA CLOUD WEBSITE: WILDFLY

The LAUDA.LIVE IoT platform website is hosted using an Azure Webapp Service. This is a mature framework that guarantees fast deployment, scalability, and updates based on Java. It is especially well fitted for Cloud applications with a large community supporting and evaluating it.

Access to the LAUDA.LIVE requires a validated user, since all the new users are evaluated by the LAUDA staff. The website is adapted to each user's permissions, which are granted at different levels (user, user rights, organization, device, etc.) for maximum customization and for security and safety reasons.

User authentication and sign in is realized by built-in authentication feature for App Service and Azure Functions from Microsoft with Microsoft Azure AD as Identity provider, the service is fully independent from the LAUDA.LIVE IoT platform and increases the security. The webserver uses the authenticated user to provide access to the IoT platform restricted to the dedicated user and device permissions.

Currently only the LAUDA Service employees will have access to the LAUDA device data to perform the LAUDA Remote Support Service.

Finally, all write and edit functions are restricted by user rights and require a Multifactor Authentication (MFA). This MFA can be used from different applications in your smartphone (i.e., the Microsoft Authenticator or Google Authenticator) since it is based in the Time-based One-time Password algorithm. This approach is a standard defined in the RFC 6238, proven to be an effective way of protecting websites against malicious intents to steal accounts.

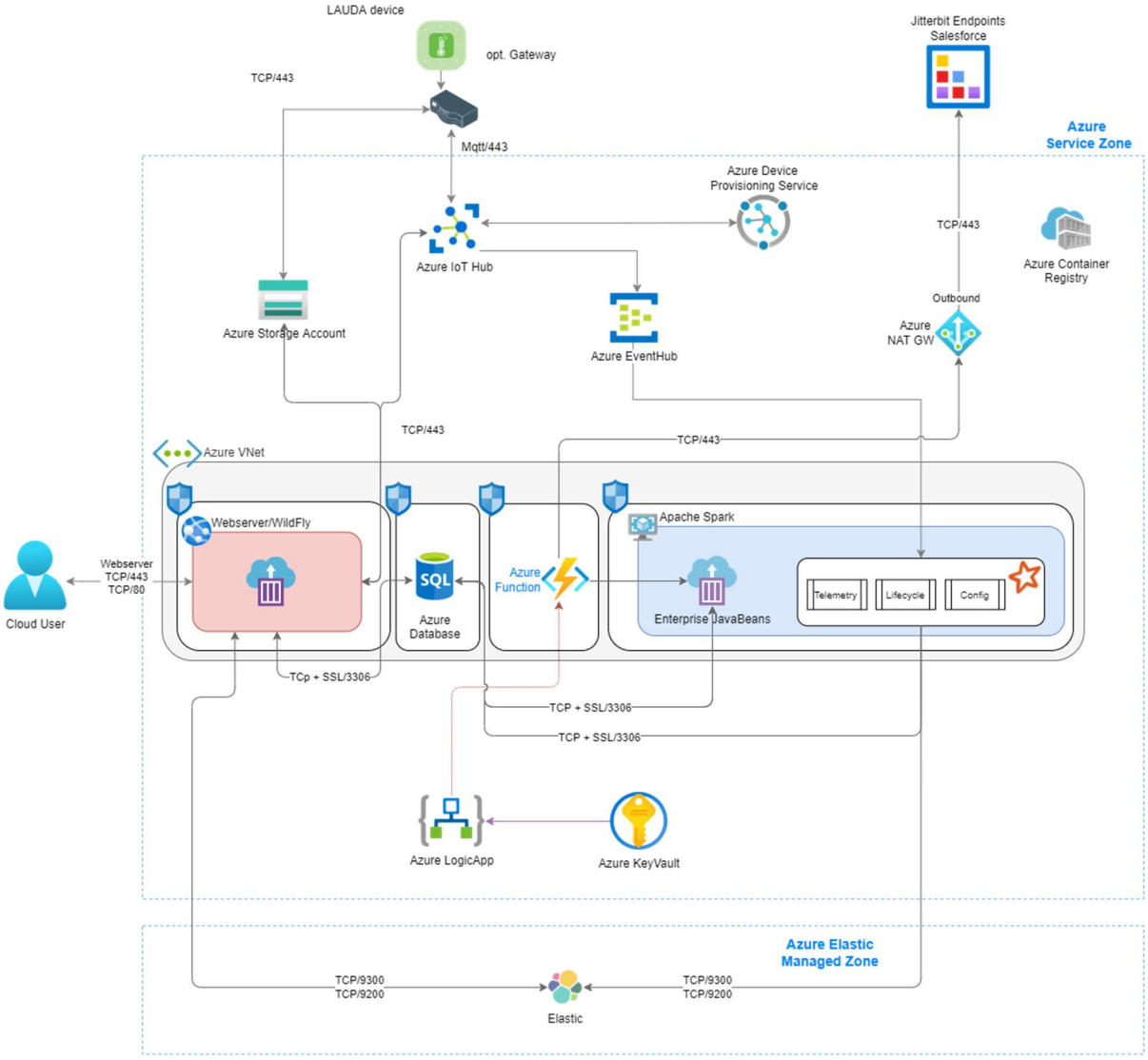

Figure 1 LAUDA.LIVE IoT Platform Overview