Solution Overview

Connected Urban Transport

159 35-HSC 901 40 Uen Rev B

Contents

1 Introduction

1.1 Document Purpose

This document provides an overview of the Connected Urban Transport (CUT) solution. The CUT business case is outlined and the CUT functionalities that support the business case are described. The CUT architecture is presented at a high level.

1.2 Document Scope

The document is structured in the following way:

- Chapter 1- Document introduction
- Chapter 2- CUT Business Context outline including solution goals and objectives
- Chapter 3- CUT Business Services description
- Chapter 4- CUT Functional Component description
- Chapter 5- Expansion of the Business Service description through sample Use Case presentation
- Chapter 6- CUT Technical Architecture overview
- Chapter 7- Security and Privacy
- Chapter 8- Onboarding
- Chapter 9- Reference documentation for further reading
- Chapter 10- CUT Terminology document reference and table of Abbreviations used in this document.

1.3 Target Audience

This document is intended for all readers wishing to gain an overview or introduction to the CUT solution and its potential. It is particularly suitable for Account Managers, Product Managers, Solution Architects, System Engineers and Business Analysts.

2 Connected Urban Transport

2.1 Market Context

Transportation is an integral part of our society. Over the last decade, the transportation landscape has evolved tremendously.
Despite this, cities and transportation authorities struggle with the operational responsibilities of existing infrastructures and with planning for future technology evolution and infrastructure expansion.
Cities and transportation authorities have become the owner of many different systems, delivered by many different suppliers, over time. However, exchange of data across systems is lacking, thus making infrastructure management cumbersome and time-consuming.

The CUT solution transforms this model by providing a platform to centralize orchestration of the independent infrastructures.

2.2 Solution Goal

The key Business Principle behind CUT is the drive to collect, present and act on real-time asset data from diverse systems, in order to streamline management, furnish intelligent insights and support automation.

2.3 Solution Summary

CUT provides secure, centralized control of diverse, external transportation systems. CUT allows co-ordination across infrastructure groups by providing an overlay on top of separate data silos and linking the available data in real-time. Example infrastructure asset groups that may be coordinated centrally from CUT are traffic signal controllers, cameras, school flashers, digital message signs and related assets such as street lights, bus traffic management systems and parking applications. CUT provides I2X (Infrastructure to anything) and is an important component in the evolution towards cooperative, connected and automated vehicles.

Each external system is easily integrated in a way that exposes the underlying system assets (devices) to the CUT User, allowing them to visualize and manage the assets. Asset visualization is achieved through the CUT GUI, a sophisticated tool to centralize operational tasks. The CUT GUI provides the over-arching view of all the stand-alone system assets in one browser. Asset control through targeted command execution is built-in. The webpages of the stand-alone asset systems may also be launched from within the CUT GUI.

As a broker of information, CUT exposes interfaces (APIs) which allow access to the assets and asset data for trusted external systems or applications, in a secure and controlled manner.

CUT is a driver of Automation. Through use of a powerful Rule engine, CUT triggers actions based on pre-defined events that are detected from the continuous stream of asset data, as it manifests. Secure, real-time command and control across silos is provided with permission-based access control.

2.4 Solution Concepts

The key concepts behind the CUT solution are as follows:

- CUT software, comprising the CUT GUI and CUT API suite is deployed in the Cloud as-a-Service (aaS).
- CUT is based on the Ericsson Internet-Of-Things (IoT) platform that separates the application logic from the generic IoT solution capabilities and which minimizes integration work.
- CUT uses Microsoft Azure Cloud to provide Cloud services such as Virtual Machines (VMs) for the CUT solution and user Authentication through Azure Active Directory, amongst other benefits.
- CUT secures User access to the solution through centralized identity management (Authentication and Authorization) coupled with a Role-driven approach to restrict access to specific asset groups and CUT tasks. Access controls apply to external users of the CUT interfaces (APIs) as well as to CUT GUI Users.
- CUT provides development tools, APIs, and a collaboration environment for ecosystem partners which enables new business to develop, test, deploy, and integrate efficiently.
- CUT follows a continuous integration (CI) and continuous deployment (CD) cycle to ensure feature improvements are available in the latest version.
- CUT supports the customer to apply the CUT functions in a manner tailored to their needs. Ericsson deploys the CUT instance in a process called Onboarding which takes the customer needs into account, including integration with the customer's independent asset groups (3PPs).

3 CUT Business Services

CUT is primarily designed as a broker of information and actions, by connecting information producers (devices or applications) to information consumers (end-users) in a secure, controlled manner. CUT is a real-time, dynamic data exchange that goes beyond traditional brokering to allow personalized insights triggered by data values that are according to user configuration.

The two types of Business Services provided by CUT may be seen as Information-based and Control-based. The figure below illustrates the overall concept.

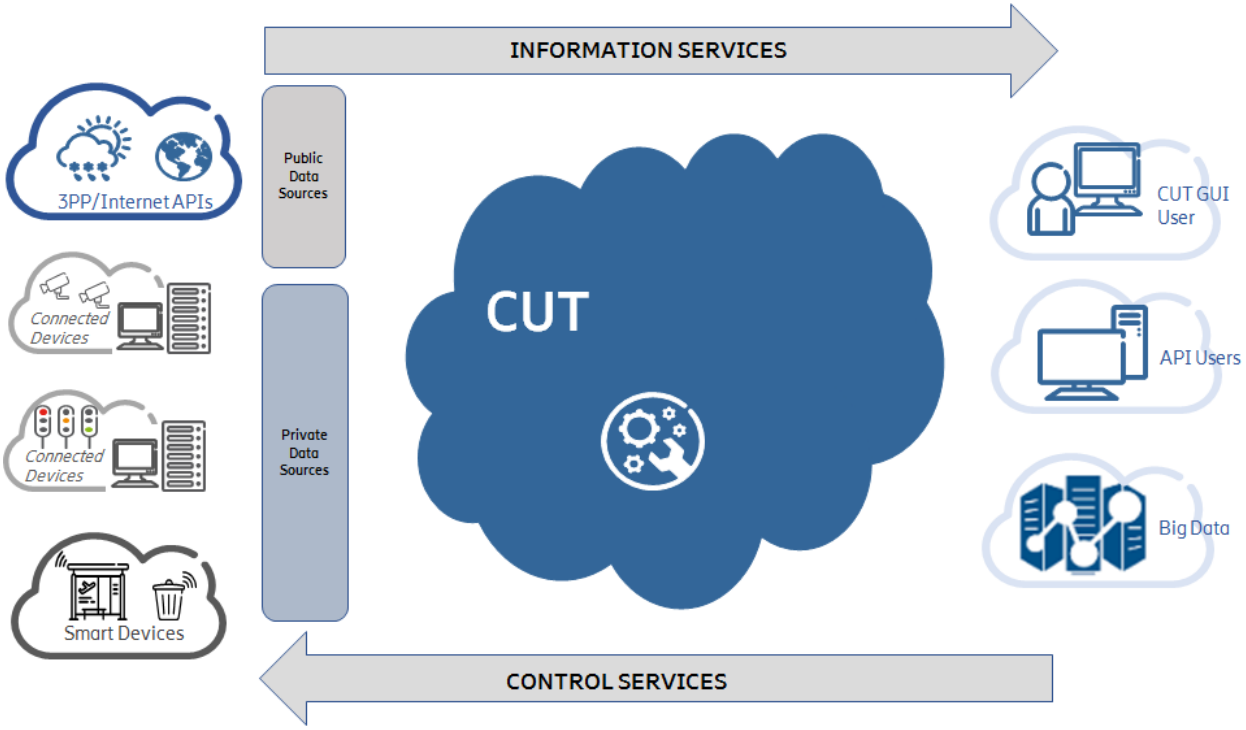


Figure 1: CUT Business Services Overview

Examples of CUT Information Services are

- Presenting the transportation assets on a map, in real-time, through the CUT GUI for Traffic Management
- Fetching asset data from a Southbound (3PP) Application that handles connected devices, via the CUT APIs
- Pushing Personalized Insights towards the CUT GUI User at logon based on pre-defined Rules
- Providing CUT data in bulk for processing by a Big Data solution (oData)

- Providing Role-based access to ensure that CUT GUI Users only have access to the data and tasks for which they have permissions (Identity and Access Management)

Examples of CUT Control Services are

- Applying Actions towards a specific asset (device) using the APIs of an external application (Application Linking)
- Launching specific, external (3PP) webpages (Deep Linking)
- Supporting Rule and Event creation to automate Actions towards assets and drive personalized (User) insights

Detailed examples of the Services can be found in Chapter 5.

4 CUT Functional Architecture

The CUT platform is highly modular, which allows for Ericsson and 3PP components to be utilized as needed. The figure below shows the CUT functional architecture at a high level.

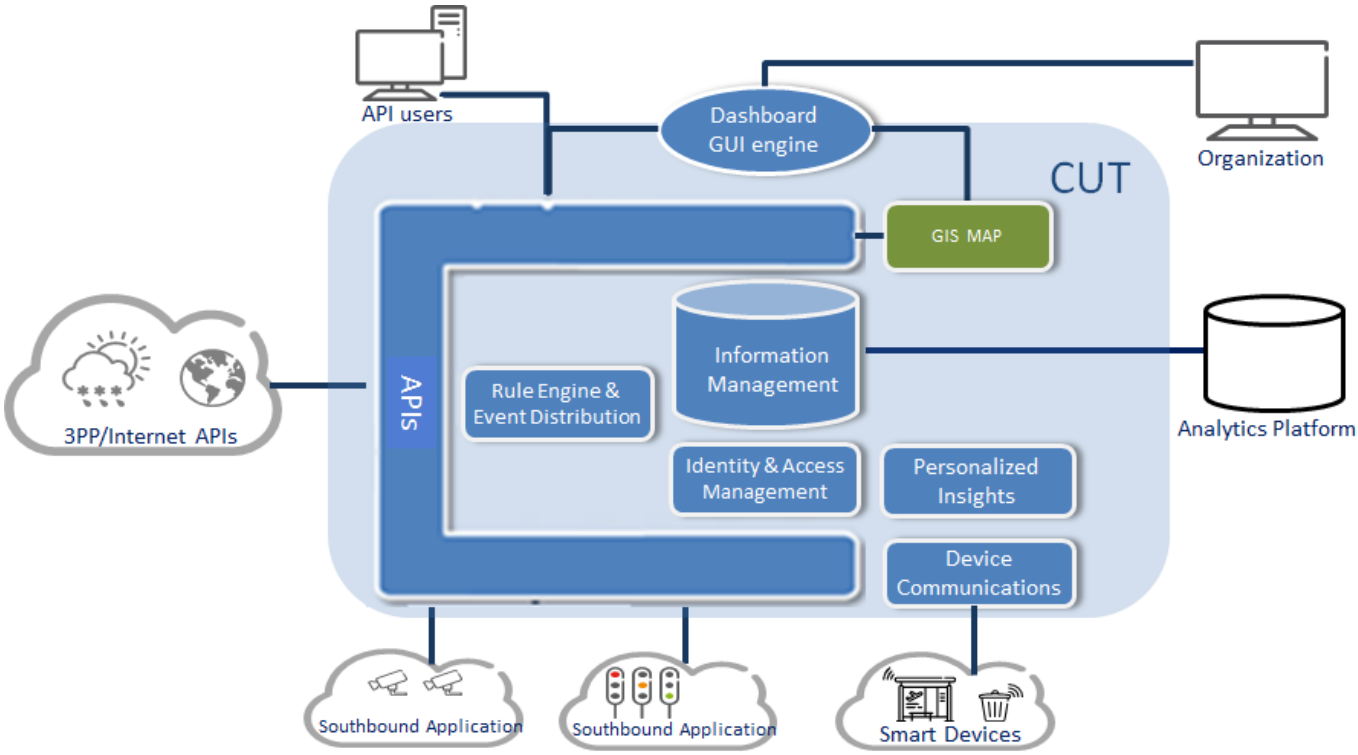


Figure 2: CUT Functional Overview

4.1 CUT Functional Components

4.1.1 Identity and Access Management

Identity and Access Management is integral to the use of CUT and precedes all CUT User API requests whether from an external application/device or from the CUT GUI.

Authentication is handled by Microsoft Azure cloud services while Authorization is handled by CUT. More information on Azure may be found in Ref [8]. CUT provides Role-based access management for Authorization, but access can also be provided on an individual basis. By assigning Users to one or more Role(s) and providing tailored information to a specific Role, a flexible manner of Access Management can be achieved. Authentication and Authorization are discussed further in section 7.2.

CUT Identity & Access Management also supports Single Sign-On (SSO). With SSO, an authorized User logs on once and is then granted access to all applicable 3PP applications without having to re-enter their credentials.

4.1.2 Dashboard GUI Engine

The CUT GUI provides the End User interface in a dashboard view. It enables use of background Maps and overlays this base Map with icons representing devices (assets), according to the User permissions. The CUT GUI may be configured by the User according to need and these preferences are stored and maintained in the CUT database. More information can be found in the CUT User Guide, Ref [1].

The figure below shows an example view from the CUT GUI.

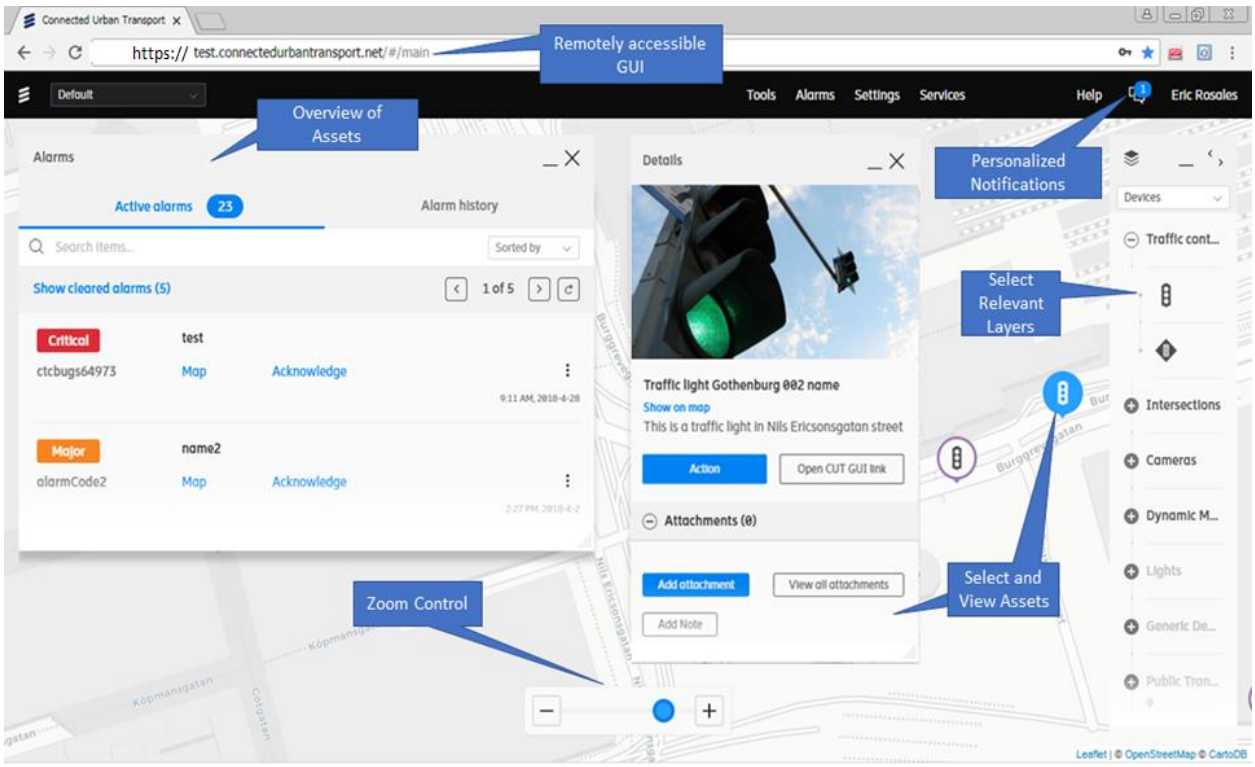


Figure 3: CUT Dashboard GUI- Example Screen Shot

4.1.2.1 Deep Linking

Deep Linking allows the CUT GUI User to redirect to the webpages of a Southbound Application (3PP sub-system that manages a set of devices, such as a set of roadside cameras) from the CUT GUI. CUT invokes the Southbound Application webpages through URL invocation. SSO-credentials may optionally be used to Authenticate and Authorize the User's request.
Note that while Deep Linking is often used to invoke webpages of a Southbound Application, it may, in fact be used to launch any relevant, allowed webpage. By enabling seamless switching between applications, Deep Linking further supports the orchestration role of CUT as the User can efficiently pull up specific websites to deep-dive into details for troubleshooting, configuration and so on.

4.1.2.2 Application Linking

Southbound Applications may expose a set of actions that can be triggered via its own REST APIs. Such an application is said to be a Linked Application.

Application Linking is extremely versatile, enriching the action capabilities of CUT. Invocation of the Linked Application API is either manually, by a User-triggered action from the CUT GUI or an automatic action triggered by a User-defined Rule, configured in CUT. Thus, it is a key component in Automation. Please refer to section 4.1.6 for more information on Rules.
Application Linking is detailed in section 5.2.2, Use Case, Device Configuration.

Note that while Application Linking is most often used to trigger the APIs of a Southbound Application managing certain devices, it may, in fact be used to call any relevant, allowed REST API. That is, the called application does not have to be device-handling. The Use Case in section 5.2.1 illustrates an example of linking to a non-device application.

4.1.3 GIS MAP

Geographic Information System (GIS) and MAP are separate functionalities, which are often combined. They are used by CUT to present the graphical map and related assets to the User.
CUT is not tied to use of a specific GIS or MAP provider. Map Providers can be supported if required or customer in-house products.

The MAP component provides a scaled, geographical representation of the real world for use mainly as the CUT GUI background. The GIS component is an advanced database that stores information in a geographically coded manner. It provides geolocation-related functions such as location referencing, geo-coding, map matching and so on.

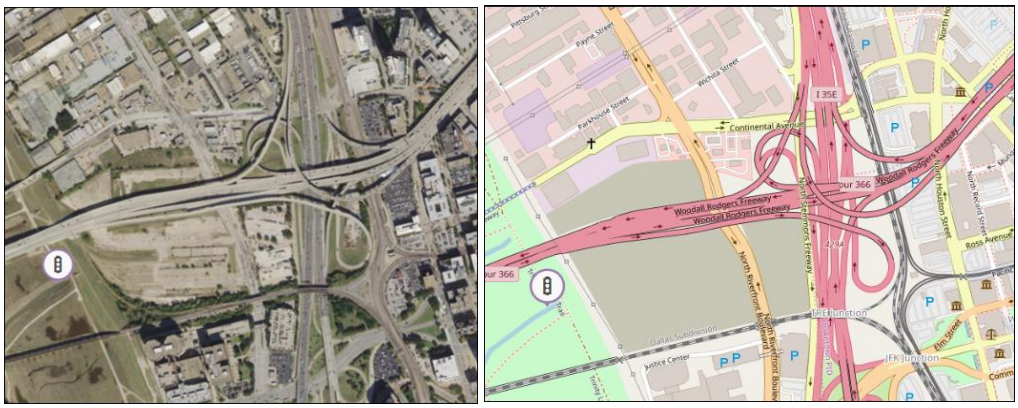


Figure 4 Different MAPs of same area-Example Screen shots

4.1.4 Device Communications

Connected devices are typically connected in a device-specific cloud, and inter-connect with CUT via the CUT APIs used by a Southbound Application.

4.1.5 CUT APIs

Use of the CUT interfaces is governed by REST APIs. APIs provide a set of rules, protocols and conditions on how to access and use the CUT data and functions. The CUT API is used, for example, by the CUT GUI component to request data on behalf of the End User.

The CUT API is also used for interaction with Southbound Applications e.g. a traffic-signal controller management application.

CUT REST APIs are provided as online Swagger documentation to provide detailed support for developers. Please refer to the CUT Interface Description, Ref [5] for more information.

4.1.5.1 CUT Adaptors

If the protocols of CUT and the Southbound Application sub-system are incompatible then a CUT 'Adaptor' is developed and deployed for these integrations. The Adaptor acts as a protocol converter between the API published by the Southbound Application to the API required by CUT. The need for an Adaptor is established during the start of CUT Service Onboarding process. Note that an Adaptor, if needed, may be created by either Ericsson or the Southbound Application vendor.
More information can be found in the Southbound Application Integration Guide, Ref [9].

4.1.6 Rule Engine & Event Distribution

Rules may be set so that an Action is triggered following a pre-defined Event (threshold breach by a device measurement).

For each Device Type (group of similar devices from the same vendor), an agreed set of possible Events is defined by Ericsson, during Onboarding. The Events specify what measurements can be expected from the devices within the Device Type and what constitutes an unacceptable measurement threshold. What Action that could apply when measurements are exceeded is also identified. When the User creates a Rule for a Device Type in the CUT GUI, the available measurements and Actions that were agreed are made available for selection. Actions could be 'open configuration web page' (Deep Linking) or 'reboot device' (Application Linking), for example.

Additionally, all the sensor data available from the Device Type is made available through the CUT GUI for Advanced Rule definition. This allows the User to leverage their personal insight to create very tailored Rules.

Note that Actions to be triggered by a Rule can vary considerably depending on the sophistication of the underlying applications. Some Actions are applicable to all Rules such as sending an email to the User or multiple Users. Other Actions might involve Application Linking where a REST API is invoked on the related device's Southbound Application, where capabilities exist.

4.1.7 Personalized Insights

Personalized Insights are tied to Rule creation.

A CUT GUI User will use their own personal insights to create rules for the CUT application. These Rules can either trigger automatic actions or send notifications to end-users. When a Rule delivers a notification to an End-User, it means that the User is receiving personalized insights, as it notifies the User that the threshold(s) that were defined have been exceeded.

The figure below shows an example of the CUT GUI Notifications window, with alerts. The User can see that new Notifications are available from the blue badge in the CUT GUI Navigation Bar, as shown. In the blue badge a number is displayed, which represents the number of new Notifications for the User. The User clicks on the blue badge and the Notifications window opens.
Note: The Use Case Personalized Insights is described in section 5.1.2.

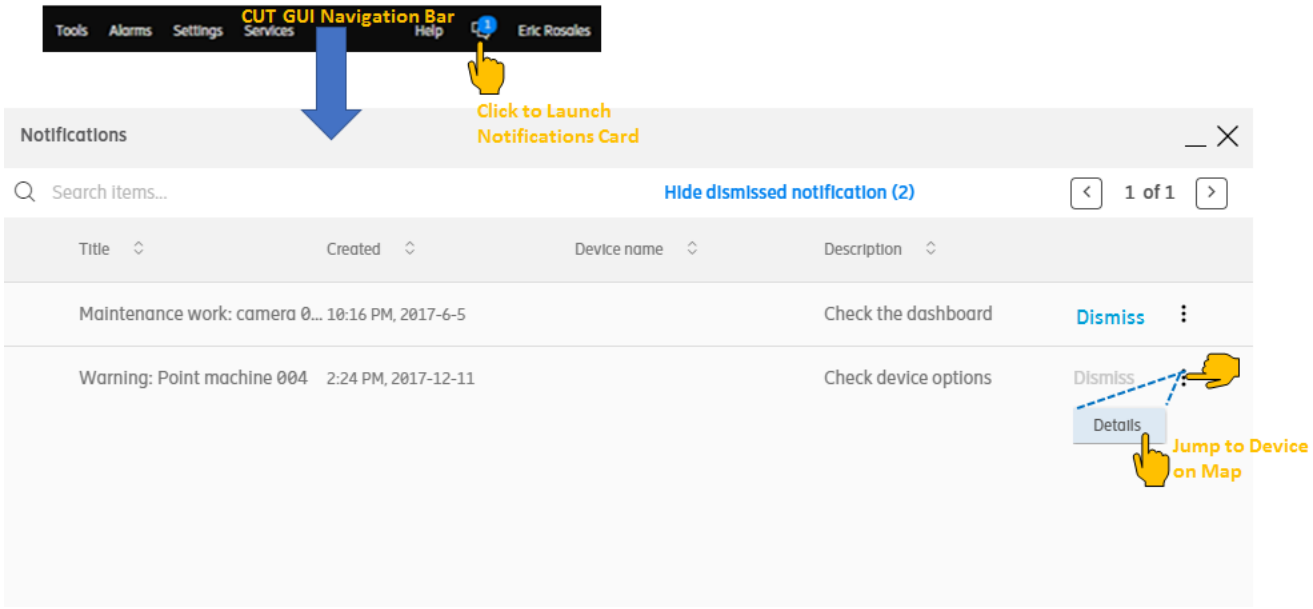


Figure 5 Personalized Notifications in the CUT GUI-Example Screen shot

It is expected that users will first want to trigger notifications prior to configuring automated actions to insure the conditions for triggering are properly configured.

4.2 CUT Interfaces

The figure below shows the CUT interfaces and principal actors within the CUT solution. The interfaces and actors are described below the figure.

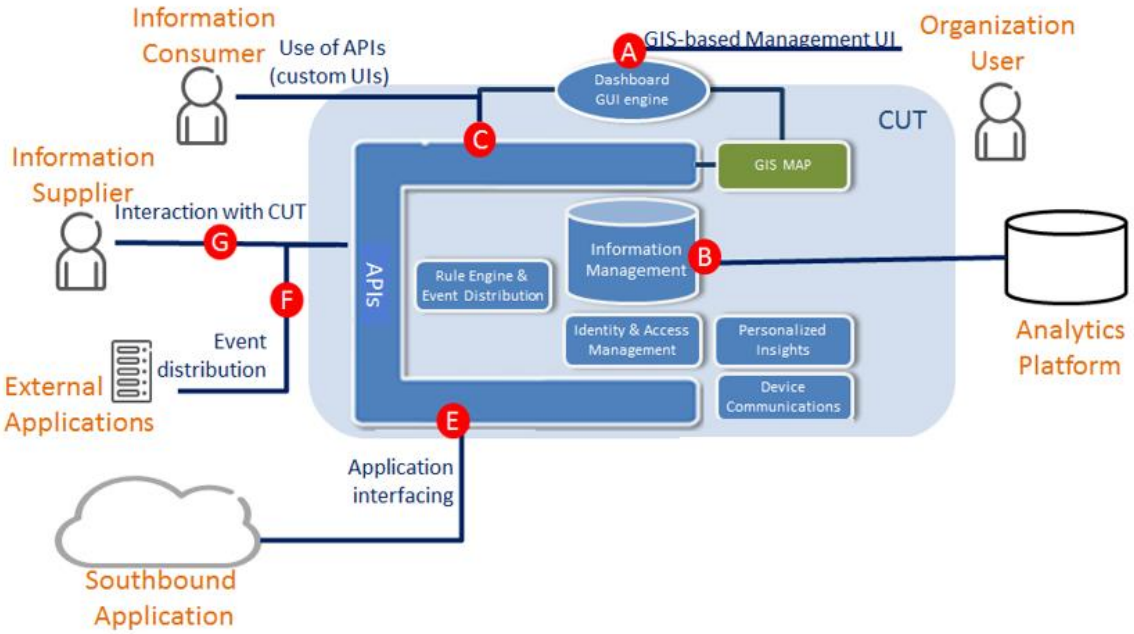


Figure 6: CUT interface overview

4.2.1 A Interface- CUT GUI User

This is the human-to-machine interface used by the CUT User to interact with the CUT-supplied Dashboard GUI or, alternatively, their own custom-deployed UI that accesses CUT functionalities via the exposed CUT APIs.

The CUT GUI User receives a dashboard-view of the traffic management devices available in CUT, may view private data published into CUT, drill down into device information and control automatic event distribution via the Linked Applications functionalities. More information on the capabilities of the CUT GUI may be found in the User Guide, Ref [1].

Note that the CUT Dashboard GUI itself uses the same APIs ('C' in the figure above) that are used by other, external Information Consumers over a machine-to-machine interface.

4.2.2 B Interface

CUT supports interface which allows for the transferal of stored device data to an external system for analytics and further processing.

4.2.3 C Interface- Information Consumer

The Information Consumer is any actor that makes use of the exposed CUT APIs.

Most Information Consumers are external users of the system, which are only granted access to the APIs specified by contract with the CUT solution owner. They are not users of the CUT Dashboard GUI. The CUT GUI itself however, is an Information Consumer and is an internal user of the system.

Information Consumers typically use the CUT APIs to create their own applications on top of CUT. The API is a REST-based API that is accessible via HTTPS. Authentication and authorization credentials are required from the Information Consumer and are built-in to the API specification. CUT can restrict the Information Consumer's use to specific APIs and also apply policies for the API consumption

More information on this API can be found in the CUT Interface Description, Ref [5].

4.2.4 E Interface- Southbound Application

The E interface allows CUT GUI Users to link to external, Southbound Applications for management of a Device Type (group or cloud of alike devices) through the exposed CUT APIs. The E interface is used by the Southbound Application to feed the device data into CUT.

An example of a Southbound Application would be the video management system that controls a set of traffic cameras. The Southbound Application typically has its own API that is either compatible with CUT or requires an Adaptor (please refer to section 4.1.5.1).
Further information on integrating a Southbound Application may be found in Ref [9].

Note: A Southbound Application may also be invoked by CUT through the F interface. The E interface is solely for communication through the CUT APIs.

4.2.5 F Interface- Application Linking/Deep Linking

Some (Southbound) Applications expose a set of actions that can be triggered via their own REST APIs. This is called Application Linking. Deep Linking is where the CUT GUI User may launch a specific webpage.

The F Interface in CUT provides the following:

- Application Linking: It allows for CUT to make an API call to any external application using that application's own REST API
  This is typically used for the purpose of invoking Actions directly on a device via a Southbound Application's own APIs

- Deep Linking: It allows for the CUT GUI to launch webpages of an external application (typically a Southbound Application) on behalf of the CUT GUI User in the User's web browser
  The webpage(s) launched are typically those of Southbound Application but do not have to be.

A description of Application Linking may be found in section 4.1.2.2 and on Deep Linking in section 4.1.2.1.

4.2.6 G Interface – Information Supplier

The information supplier is an organization or service that feeds additional information to CUT via the APIs. As with all CUT API requests, the Information Supplier (application) is first Authenticated and Authorized before publishing to CUT is allowed. Example uses of this API Functionality include:

- Inventory support: synchronize the device inventory from the supplier's master database to the slave database in CUT. Information Supplier data is used to provide information on non-managed devices and is not stored in CUT except for the caching of the last received value.

- Messages: For example, traffic messages as defined in DATEX standard. These messages are not associated with a managed device. E.g. road work or accident may be pushed to CUT via this API.

4.3 CUT Data Overview

The CUT Data Model structure is shown below. The Data Model shows the CUT data hierarchy and is indicative of the CUT data available via the APIs.

The Organization object forms the top tier of data for a CUT customer and is not accessible outside of the CUT Ericsson team. Data from the lower tiers is accessible via the APIs, provided the correct permissions are in place. Data objects outlined in green in the figure below relate to Users, User Groups, Roles. Data objects outlined in yellow relate to Devices and Services. Data objects outlined in blue relate to Events, Rules and Actions.
For more detailed information on the CUT Data Model, please refer to Ref [2].

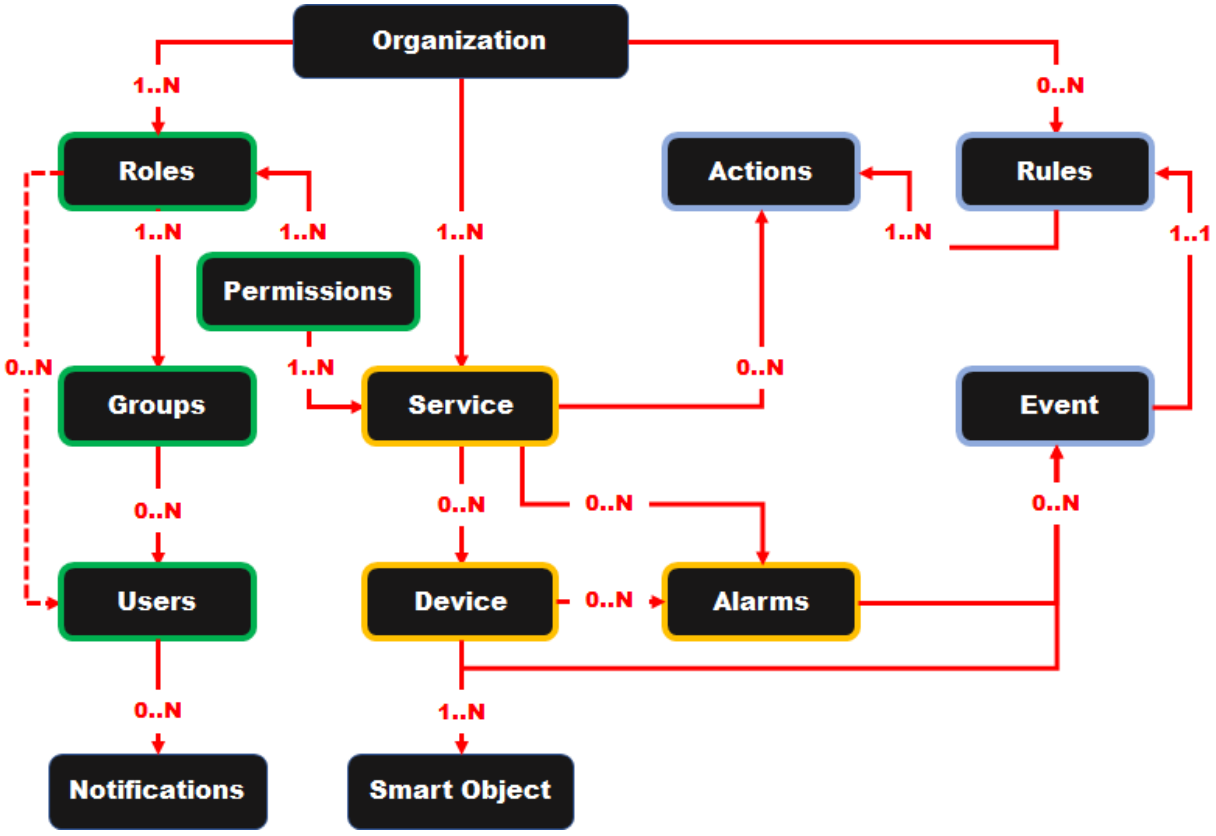


Figure 7: CUT Simplified Data Model

4.4 CUT Function mapping

The figure below shows the mapping between the CUT functional components and the underlying technology.

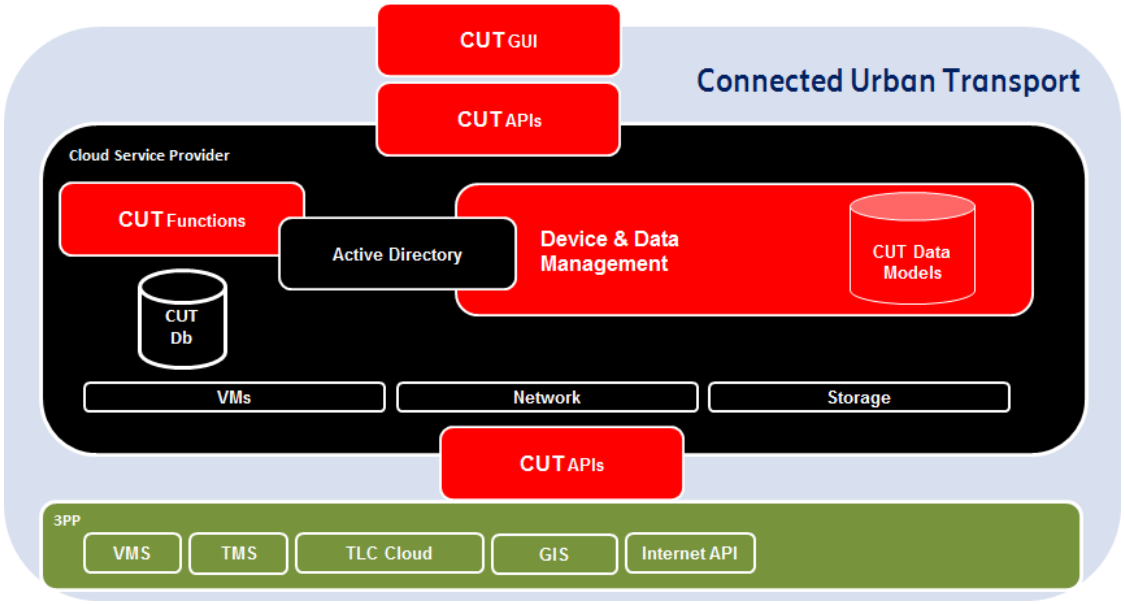
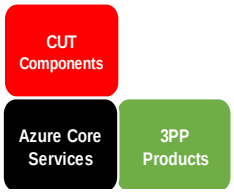


Figure 8: CUT Solution Architecture

Key:



As shown, the CUT solution consists of a combination of Ericsson CUT and components hosted in the Microsoft Cloud. The customer's Southbound Application vendors (3PPs) complete the solution.

The CUT API is used for communication with the Southbound Applications (3PP systems) such as Maxview from Intelight, a traffic-signal controller application. Where required (where protocols don't match) a protocol converter called an 'Adaptor' can be deployed for these integrations.

5 Use Cases

This chapter describes example use cases that can be realized with CUT.

The CUT application can be configured to interwork with Southbound Applications via CUT APIs, Deep-Linking or Application Linking. The Actions discussed in the use cases are examples of interworking visualization in the GUI. These Actions can be configured to be invoked from the device details card in the CUT GUI (enabled by Ericsson at Onboarding) or via a rule by the CUT User.

5.1 Information services

5.1.1 Traffic Management Overview

This use case outlines use of CUT by a Traffic Management Center Operator to view a particular set of assets on the map of their region and then display the details of a specific asset (device). Situational awareness across device types such as traffic signal controllers, cameras or digital message signs enable the Traffic Management Center Operator to quickly decide where to prioritize efforts in order to maximize the efficiency and experience for citizens, visitors and commerce. This Use Case is an example of CUT interacting with the device-handling Southbound Applications over the CUT APIs.

The figure below depicts the steps required to execute this use case. The steps are detailed below the figure.

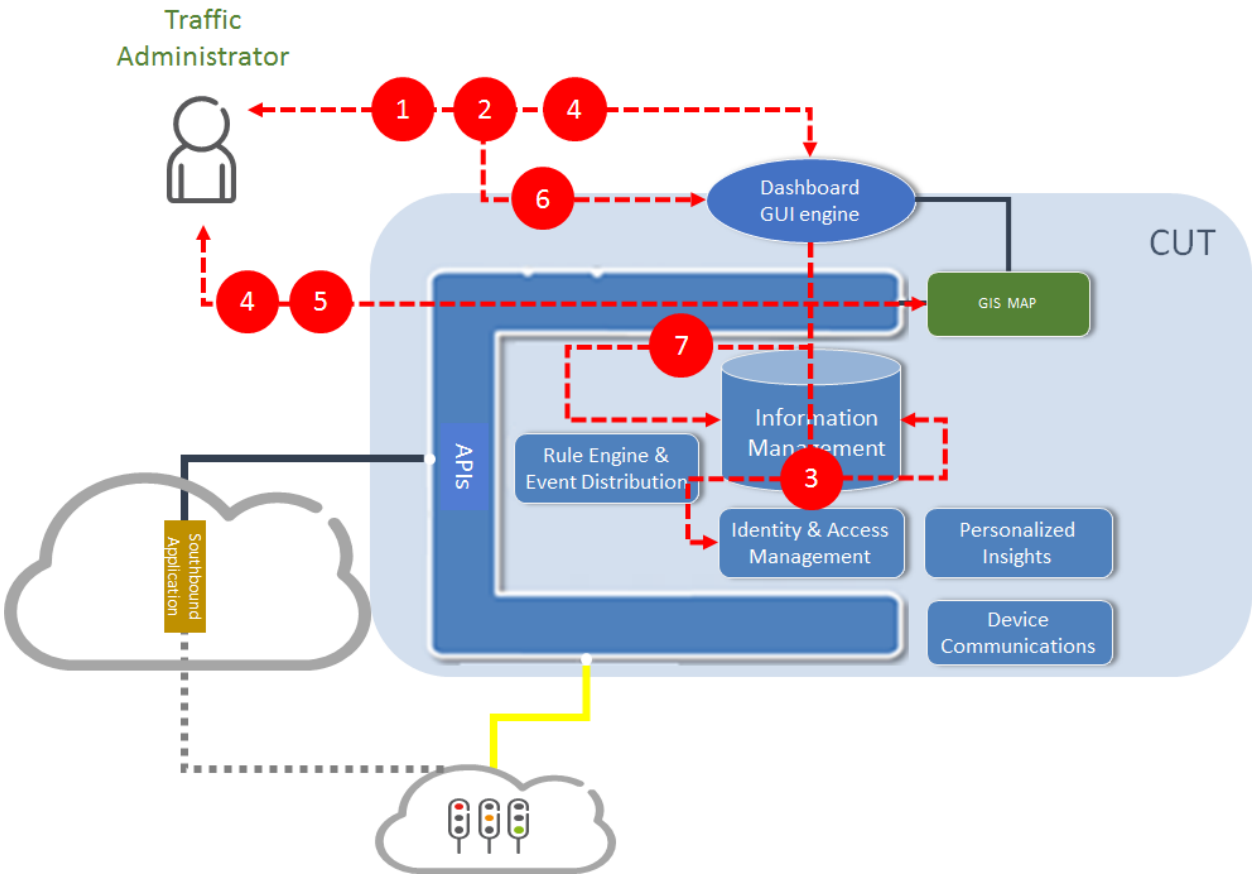


Figure 9: Traffic Management Overview

Steps:

1 The Traffic Management Center Operator (CUT GUI User) opens a web browser and enters the URL of the CUT Dashboard GUI. They are presented with the login page.
2 The User enters their access credentials
3 The Dashboard GUI:

- Authenticates the User
- Authorizes what the User is allowed to view through the GUI based on their CUT Role
- Analyzes the User's CUT profile information to determine the default region/zoom-level for the map
- Requests the GIS/map component to present the map

4 Dashboard GUI presents the required view to the User, including all layers that are Authorized for this User as well as the alarm status of each device.
5 The User zooms and pans the map as desired
6 The User selects a specific device to access the related device details
7 The Dashboard GUI retrieves the detailed information from CUT and presents it to the User. Note that CUT presents the information it continuously retrieves from the Southbound Applications.

5.1.2 Personalized Insights through Notifications

This Use Case outlines how CUT provides Personalized Insights to the CUT GUI User. In this example, the Traffic Management Center Operator is monitoring a specific intersection and wishes to be informed if certain conditions change.

The figure below depicts the steps required to execute this use case. The steps are detailed below the figure. Note that it is assumed that the User has already logged on to the CUT GUI, as described in the previous Use Case, section 5.1.1.

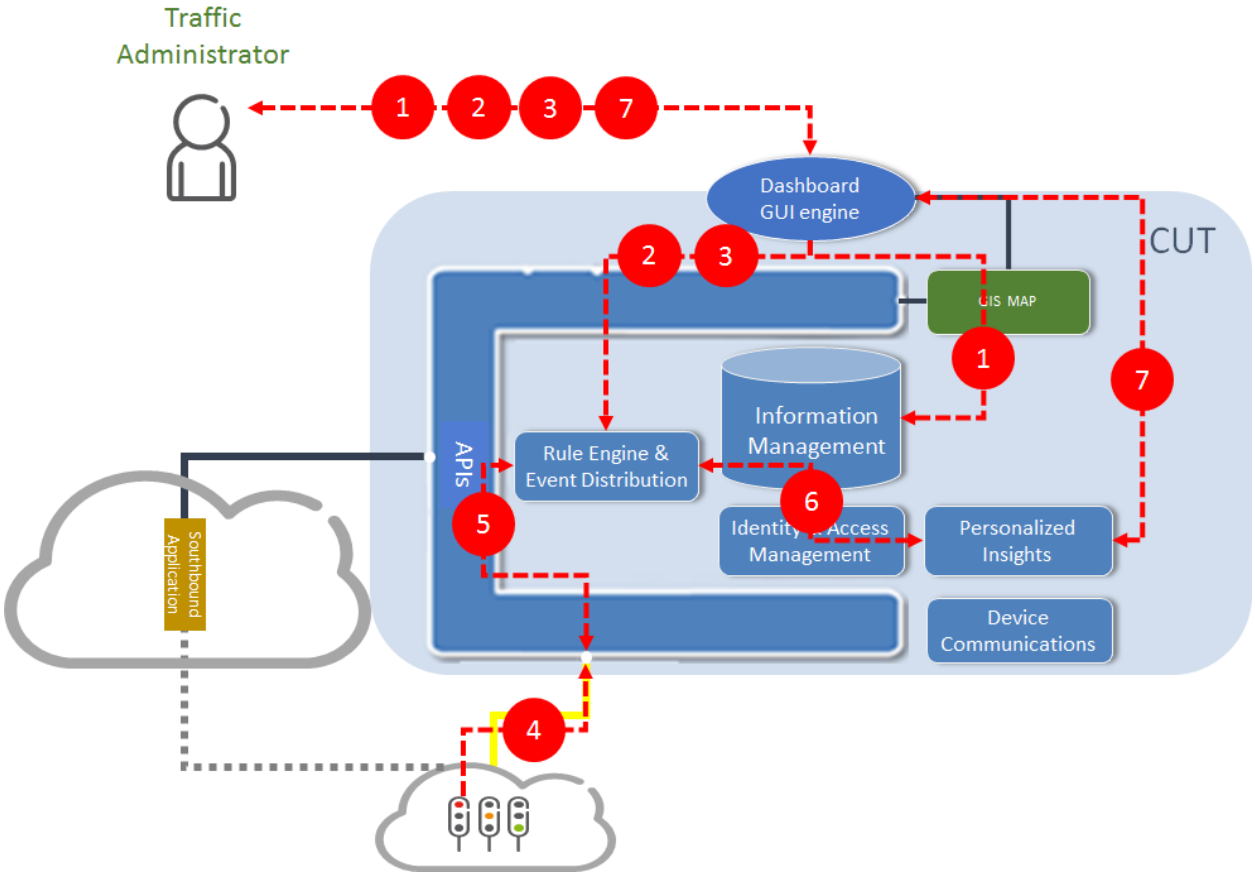


Figure 10: Personalized Insights

Steps:

1 The Traffic Management Center Operator (User) selects the device (a traffic-signal controller) that they are interested in
2 Based on the User's personal insights the decision is made to configure a specific Rule through the GUI which sets Events based on the measurements the device produces
(An example Event is if the traffic volume rises above threshold 'x' between 17:00 and 20:00)
3 The User configures the Action that corresponds to this Event to be a Personalized Notification which will be displayed in the User's CUT GUI (note that an email could also be sent)
4 The traffic-signal controller sends volume measurements to CUT

5 CUT stores the measurements and checks for active rules on the received measurement
6 If the provided measurements exceed the defined threshold and during the defined time, the defined Event occurs and triggers the related Rule which results in the defined Action occurring; a Notification is generated for the User
7 The User then instantly receives the notification in the CUT GUI. Note that Notifications persist so if the User is not logged on to the CUT GUI when the Notification is generated they will receive it at the next logon. The Notification received provides the User with Personalized Insights to the threshold breach.

5.2 Control services

5.2.1 Personal Insights driving Automation

This Use Case illustrates the automation capabilities of CUT. It is an example of Application Linking.

In this example, a traffic-signal controller reports an alarm. CUT has been preconfigured to trigger a Rule when this Event occurs. When the CUT GUI User defined the Rule, the Action *create work-order* was selected. The Action *create work order* calls an API in the 3PP Work Order application.

Note: The Work Order Management sub-system is assumed integrated with CUT, by Ericsson, at Application On-boarding. This Use Case centers on the capabilities intrinsic in the Southbound Application, the Work Order Management sub-system. In this example, the sub-system supports work order creation, via a REST API with arguments, on-demand.

The same Use Case may be applied to *any* Action that the Southbound Application can execute via its exposed REST APIs, from rebooting a device to writing a record in a database. In this example, the Work Order Management Southbound Application is not necessarily a device-handling application.

The figure below depicts the steps required to execute this use case. The steps are detailed below the figure.

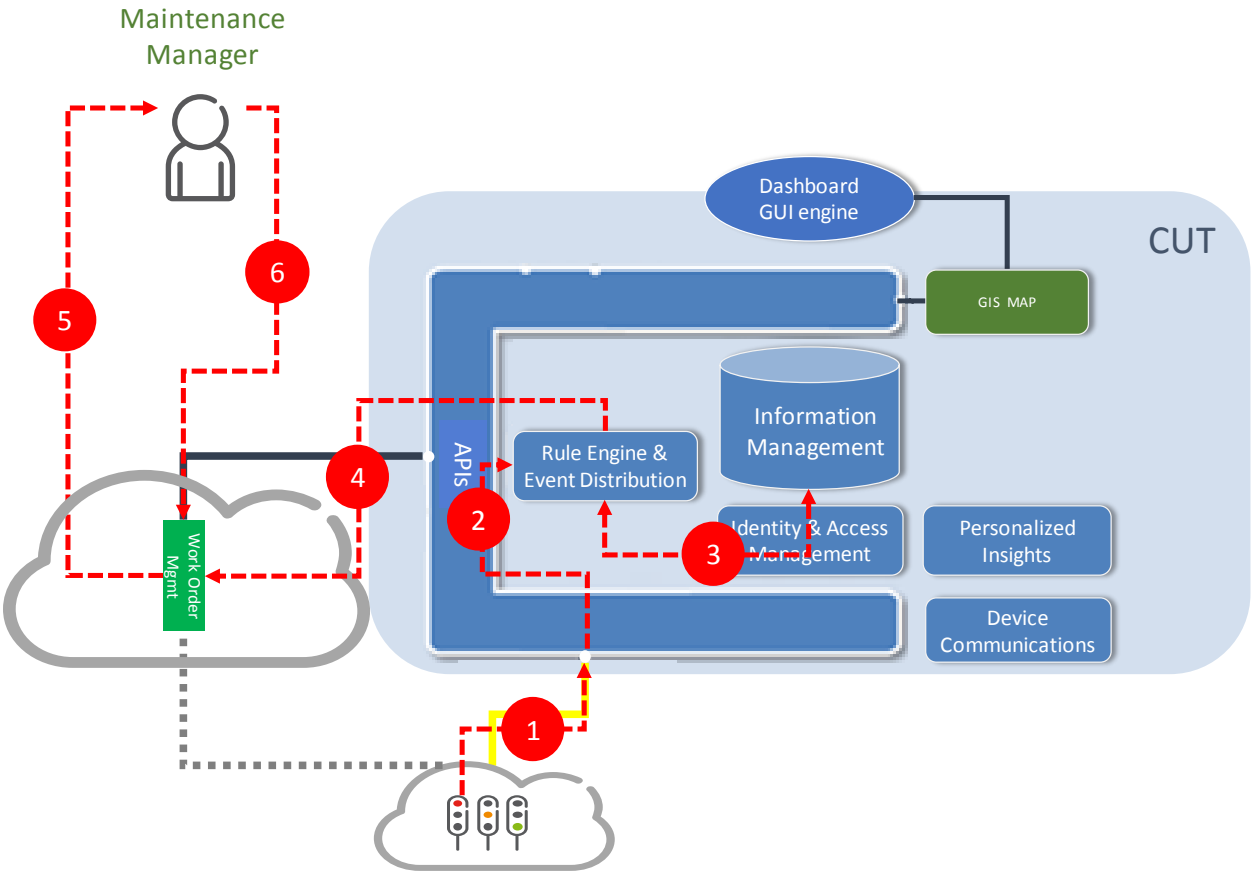


Figure 11: Automatic Work-Order Creation

Steps:

1. The traffic-signal controller reports an alarm to CUT Event distribution component
2. CUT marks the fault as an Alarm event and sends it to the CUT Event distribution component
3. Event distribution retrieves the Linked Application data for the TSC-handling Southbound Application, from central storage.
4. Event Distribution triggers the Linked Application (the TSC-handling Southbound Application).
5. Probable continuation, external to CUT: The TSC-handling Southbound Application receives the event, creates a temporary work-order and alerts the Maintenance Manager that a temporary order was created
6. Probable continuation, external to CUT: The Maintenance Manager confirms the temporary order and orders the system to create a permanent work-order and dispatches the order to maintenance team

5.2.2 Device Configuration

This Use Case outlines how an action or command may be initiated from CUT towards a specific device (asset) by launching a specific, configuration webpage. This is an example of Deep-Linking.

In this example, the Traffic Management Center Operator wishes to configure a specific device. Note that the Southbound Application that is integrated with CUT must support the required interface to launch the webpage.

The figure below depicts the steps required to execute this Use Case. The steps are detailed below the figure. Note that it is assumed that the User has already logged on to the CUT GUI, as described in the 'Overview' Use Case, section 5.1.1

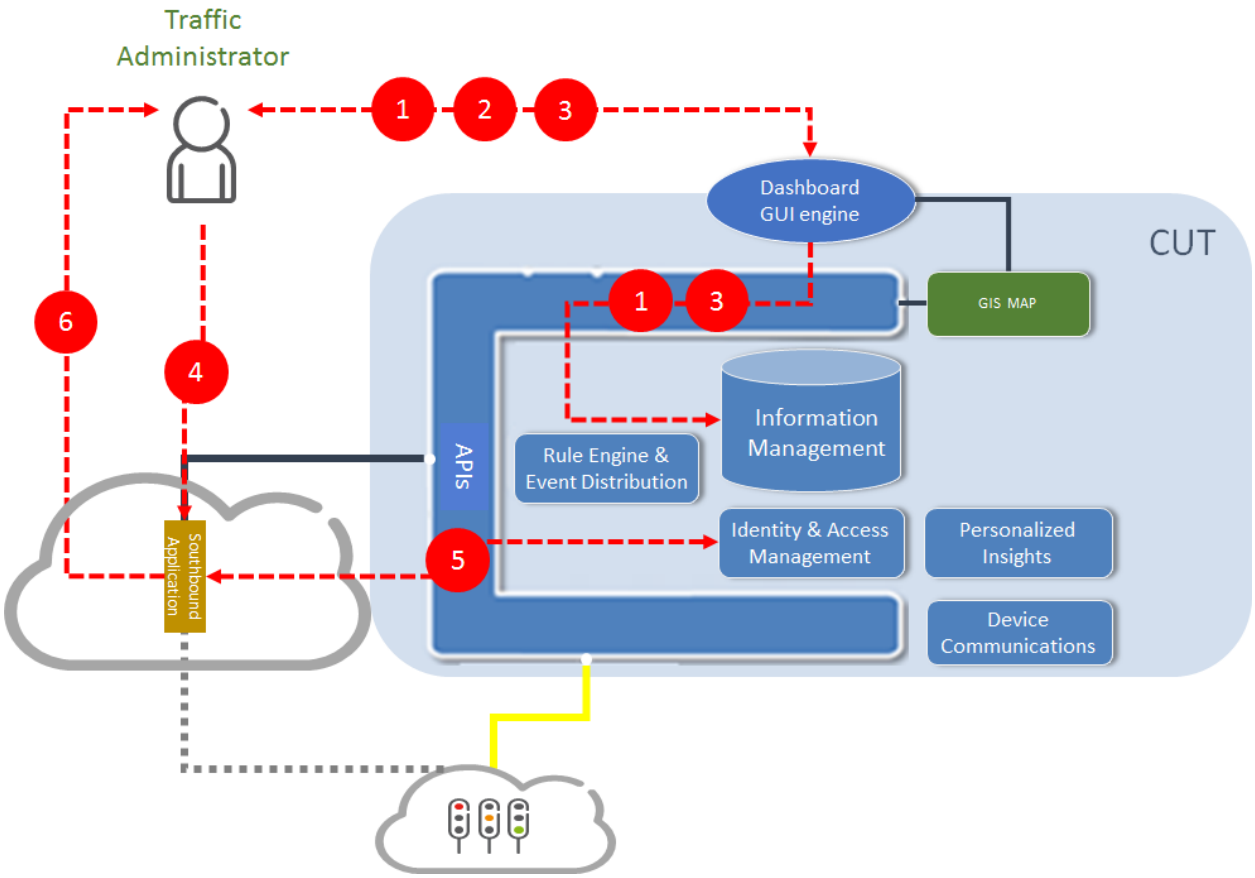


Figure 12: Device Configuration

Steps:

1 The Traffic Management Center Operator (CUT User) selects the device on the CUT GUI and opens the device details window
2 The User checks the devices details / status and determines that device (re) configuration or reboot is needed
3 The User selects the required Action (launch specific webpage) from a drop-down menu in the device details window from the CUT GUI or from the Services option in the CUT GUI Main Menu

4 The CUT GUI redirects the User's web browser to the relevant page in the Southbound Application's control GUI and includes the Single Sign On (SSO) token so the User does not need to separately logon to the sub-system
5 The Southbound Application's control GUI resolves the SSO token with CUT's Identity and Access Management function.
6 When the token is verified, access to the Southbound Application's GUI is granted and the specific configuration page is shown where the User may execute the required configuration.
Note that it is possible to modify the required configuration directly on the device if this is supported by the Southbound Application. In that case, the User would not be redirected at step 4 but instead the configuration change would be applied from invocation of the Southbound Application's REST API. CUT would still apply the SSO token verification, however. Configuration through invocation of a Southbound Application's REST API is an example of Application Linking. The basic steps of Application Linking are shown in the Use Case in section 5.2.1.

6 CUT Solution Architecture Overview

CUT is ready to serve multiple customers from a single implementation. The solution caters for simultaneous accessibility of the functionalities from multiple organizations.

The figure below shows a CUT deployment with two CUT instances; one instance per CUT customer. Each CUT instance or customer is referred to as an Organization within CUT. The whole solution is deployed in the Microsoft Azure Cloud and as shown, each Organization has its own Azure Active Directory (AAD). This is to handle Authentication on behalf of the Organization, including Authentication towards CUT. Organizations that do not have an AAD of their own can be catered for by using the CUT (Ericsson) AAD.

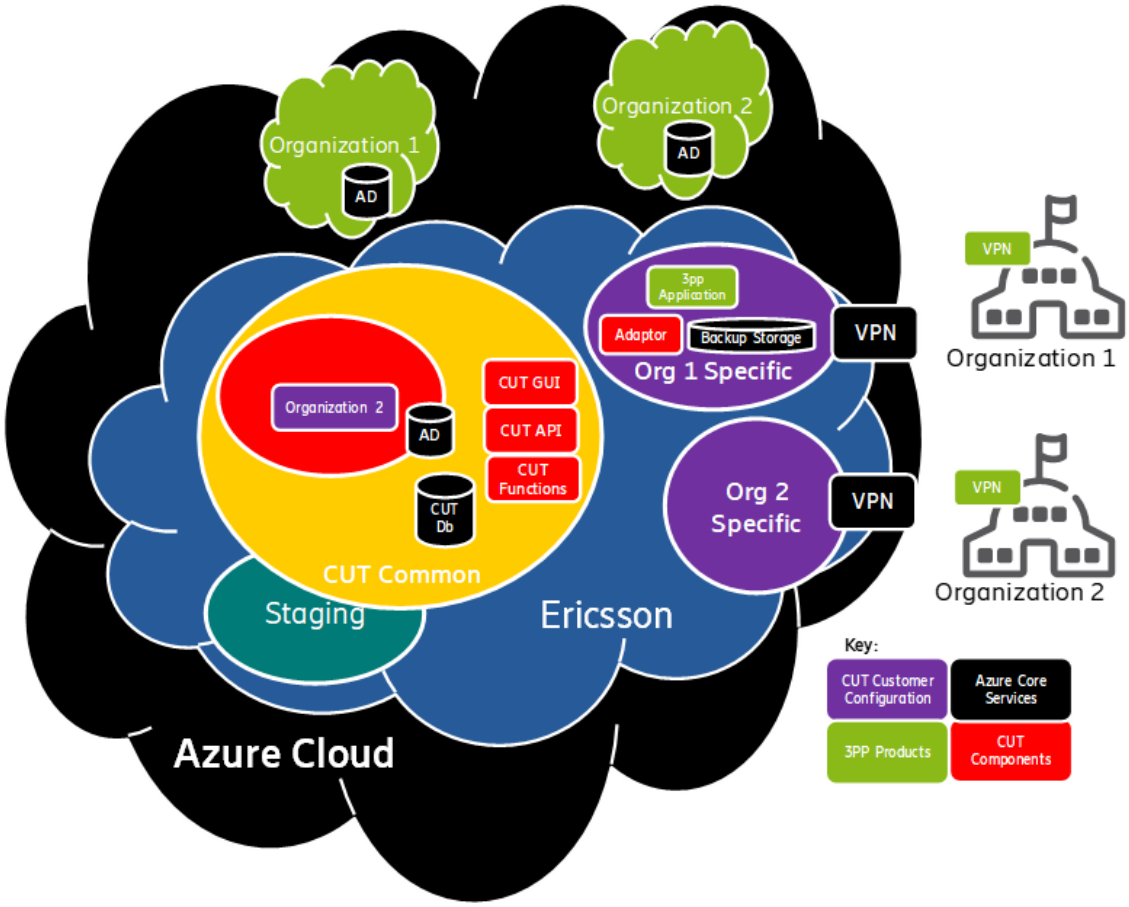


Figure 13: CUT Deployment

The CUT Solution consists of three separate environments:

- CUT Staging
- CUT Common
- CUT Organization-specific

All of these CUT environments are placed in the Microsoft Azure Cloud. The CUT Azure environment is described first, below and further sections then describe the CUT environments.

6.1 CUT Azure Environment

The default deployment environment for CUT functionality is the Azure Enterprise Cloud. However, Azure Government Clouds may also be used, upon request. All CUT components for a deployed solution instance are deployed under a single Azure subscription.

6.1.1 Access

In the diagram above, the CUT customers (called 'Organizations') connect to CUT via VPN Tunnel. Note that this is just an example of connectivity. CUT provides a public IP address and connectivity to CUT is at the discretion of the CUT customer. Redundancy is regional when deployed in the Enterprise Cloud. Government Clouds are site redundant within the specific country.

6.1.1.1 HTTPS

HTTPS connectivity is recommended, the Azure Gateway (firewall) component is used for HTTPS termination. The Azure Gateway secures the connection and then connects to the CUT backend over HTTP. In this scenario, the Azure Gateway public IP address is exposed rather than the CUT IP address.

6.1.1.2 Redundancy

The Azure Gateway is redundant and is under control of Azure management. The CUT customer is obliged to provide their own redundant connection towards Azure. Between the Azure Gateway and CUT, there is a single connection.

6.1.2 CUT Deployment

Using Azure standard offerings, CUT is deployed on Virtual Machines (VMs) with Linux Red Hat OS. NGINX webserver and reverse proxy server are deployed for the CUT GUI component. The CUT APIs are developed using javascript (JS) framework. The CUT API Application is deployed on Node JS and the related Node Package Manager (NPM).

6.2 CUT Environments

This section describes the three key CUT environments that are within the Microsoft Azure cloud:

- CUT Staging
- CUT Common
- CUT Organization-specific

6.2.1 CUT Common

The CUT Common environment contains the core CUT features and services. These features and services are shared between all customers of the CUT deployment, as shown in the figure below.

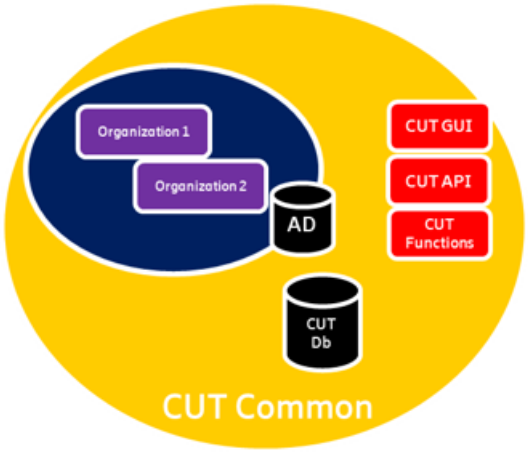


Figure 14: CUT Common Environment

The CUT Common Environment consists of:

- CUT GUI
- CUT API
- CUT Functions
- CUT Database
  Used to store data on behalf of the CUT solution and the CUT customer
- CUT Azure Active Directory (for Ericsson, not the CUT customer Organization) which is used to:
  > Link to customer-specific AAD instances (to allow single sign-on)
  > Hold end-users that do not have an AAD and other users who require access to the CUT solution (i.e. regional staff, public safety staff etc.).

6.2.2 Organization Specific

The Organization Specific environment is where specific software and services are hosted for a specific customer.

This includes, for example:

- Customer specific software (Southbound Applications if these are to be hosted by Ericsson)

- Customer specific integration Adapters (to enable the Southbound Application to interact with CUT, if needed)
- Customer specific storage
- Customer specific connectivity (VPN endpoints)

6.2.3 Staging

The goal of the staging environment is to create a “close-to-production”, fully functional environment to test new deliveries of the CUT software base-line prior to moving them to production. It can also be used to perform training or demonstration events. Typically, the customer network does not have access to the staging environment to ensure compliance with necessary security requirements.

The staging environment will consist of a minimum deployment of all the software components in the solution. Additionally, device simulators are deployed in this environment to enable full End-to-End testing.

7 Security and Privacy

7.1 General

The CUT solution aligns with NIST Guide to Industrial Control Systems (ICS) Security special publication SP800-82, "Recommended Defense-in-Depth Architecture", Ref [10].

The demarcation points between CUT and a customer is shown overlaid on the NIST Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82 in the figure below.

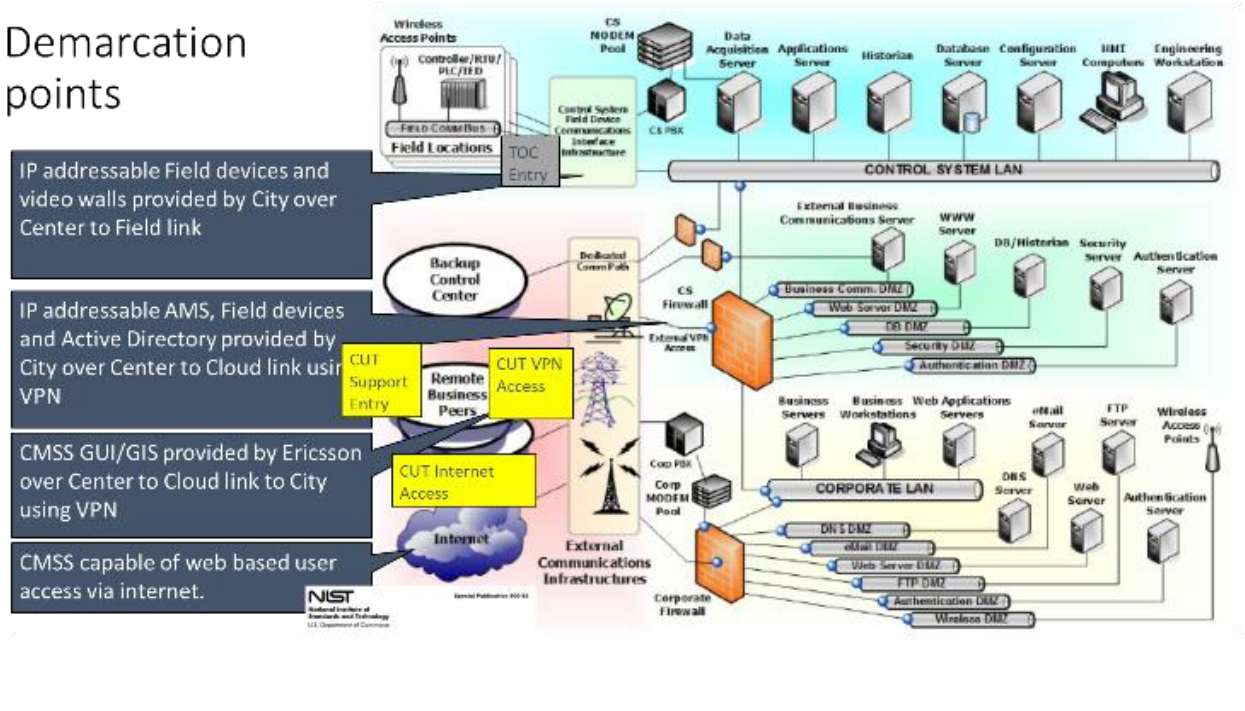


Figure 15: SP800-82 CUT

As shown in the figure, the center to field network is isolated from the Corporate LAN to restrict access to the IP-enabled devices. The abstraction of the CUT User Access from the corporate LAN means that Users can securely access the CUT GUI from anywhere, without compromise to the IP-enabled devices.

7.2 CUT Authentication & Authorization

7.2.1 Authentication and Authorization Flow

The CUT User goes to the logon URL and enters their username (email address) and password. The username indicates to Azure which Organizational AD to check. The user is authenticated in the relevant Azure AD and the Azure AD generates a token.
Azure performs a URL redirect towards the CUT backend which includes the token. The user is recognized by CUT and the token acknowledged as valid. The CUT sends the UI to the end user. The end user's GUI, which was downloaded at first logon then uses the token to request the end user GUI preferences and any data they are allowed to view via the CUT APIs. The token is valid for a configured amount of time, for example, 24 hrs. At logout, the token is automatically terminated by Azure.

7.2.2 Authentication with Azure

Authentication of a CUT user is handled by Azure. Authentication refers to verification of the CUT user credentials.

Each CUT customer (Organization) has its own cloud authentication through individual Azure Active Directories. CUT is not responsible for the Active Directory (AD) of an Organization; this management is handled by Microsoft Azure.

If an Organization does not already have an own Azure Active Directory (for example, is with Amazon Cloud or has in-house authentication) then this Organization may have its users populated in the CUT (Ericsson) AD.

7.2.2.1 CUT Users

Each CUT Organization is licensed for a number of concurrent CUT users. Users within an Organization are granted permissions to view the Organization's data via Roles which are set up by the Organization Administrator.

7.2.3 Authorization (CUT GUI)

CUT Role-based authorization controls the End-User permissions. Authorization refers to what the CUT user is allowed to view, via the CUT GUI. Roles can be fine-tuned to make the related-permissions as specific as needed.

8 Onboarding

Onboarding is the process by which CUT is deployed to a customer. Because CUT is in the Cloud the latest software is always available straightaway. This section briefly describes the Onboarding process and what's involved in a typical deployment.

Note that this Chapter focusses on initial, Organization Onboarding. Onboarding can refer to any of the following:

- Organization Onboarding e.g. each municipality
- Application Onboarding e.g. each device vendor's Southbound Application is separately Onboarded.
- Device On-boarding – This may be done by the CUT customer

8.1.1 Device and User Licenses

The first step for Onboarding a new customer is determining the number of devices and End Users that will be making use of the CUT solution.

8.1.2 Identify standard 3PP software

The next step is determining the need for 3PP software and if it is to be hosted by Ericsson. The option exists to deploy them either in the Organization's own data-center or in the Organization-specific part of the CUT cloud. These deployment options must be clarified and detailed. The options selected can have a significant impact on the Onboarding and operational costs.

8.1.3 Identify integrations

As well as selecting the 3PP software, any customer-specific integrations to CUT are identified, including Information Producers.

Typical integration examples are integration towards a non-device handling Southbound Application such as a Work Order Management sub-system or to a device-handling Southbound Application. Integration with the former could be through the Work Order Management application's own REST APIs and integration with the latter would be through the CUT APIs. Using CUT APIs may require that integration with the specific Southbound Application requires creation of an Adapter. These are typical considerations when planning CUT integrations.

8.1.4 Identify Access and Security restrictions

Also identified are the specific access and security restrictions that shall apply.

This includes specifications for the VPN connection between the Organization's data-center and the Organization-specific environment in CUT.

Additionally, Active Directory integration specifics need to be identified and clarified.

Finally, the list of CUT Users to be provisioned and the Access that they require needs to be generated. User access is driven through allocation of Roles. Each Role is defined in CUT as part of Onboarding and provides a very detailed set of permissions. Users may be allocated read, write or read and write permissions to any set of devices within CUT as well as permissions to execute specific tasks from the GUI.

9 References

Documents for further reading are listed below.

[1] CUT User Guide, 1/1553-HSM 901 4616

[2] CUT Data Model Description, 198 18-HSC 901 140 Uen

[3] CUT Terminology Document, 0033-HSC 901 140

[4] Ericsson Device and Data Management, Technical Product Description, 2_22102-FGC1013190

[5] CUT Interface Description, 155 19-HSM 901 4721

[6] CUT Terminology, 0033-HSC 901 140

[7] Microsoft Azure API Management

[8] Microsoft Azure Active Directory

[9] CUT Southbound Application Integration Guide, 1/198 17-HSM 901 4721

[10] NIST SP 800-82

10 Terminology

Please refer to the CUT Terminology document, Ref [3] for the complete list of CUT terminology used in this document.

10.1 Abbreviations

The main abbreviations used in this document are listed in the table below.

Abbreviation	Description
3PP	Third Party Product
AAD	Azure Active Directory
aaS	as-a-Service
AD	Active Directory
API	Application Program Interface
CD	Continuous Development
CI	Continuous Integration
CUT	Connected Urban Transport
GeoJSON	Geospatial JSON
GIS	Geographic Information System
GUI	Graphical User Interface
HTML 5	Hyper Text Markup Language version 5
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
ITS	Intelligent Transport System
JS	Java Script
JSON	Java Script Object Notation
LAN	Local Area Network
NPM	Node Package Manager
OS	Operating System
REST	REpresentational State Transfer
SSO	Single Sign On
TSC	Traffic Signal Controller
TMS	Traffic Management System
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine
VMS	Video Management System

Table 1: Document Abbreviations