TCS Connected Universe Platform – Frequently Asked Questions

About TCUP

What is TCUP?

[Response]:
TCS Connected Universe Platform (TCUP) is a platform that makes it easy to develop, deploy and administer Internet-of-Things (IOT) applications. It consists of a set of web services and device software modules that are specifically designed for application developers to create highly scalable, available, secure and analytics driven IoT applications. TCUP is a domain agnostic platform that allows IoT applications to be built for virtually any devices/sensors and virtually any business domain.

What are the main technology challenges addressed by TCUP?

[Response]:

- ✓ **Managing Device Diversity and Interoperability -** In an IoT scenario, we expect data in various formats and structures from a wide variety of devices, instruments and equipment sourced from diverse device vendors and OEMs. TCUP makes it easy for applications to interface with a wide variety devices and sensors.
- ✓ **Integrating Data from Multiple Sources -**TCUP makes it easy to build intelligent context aware IoT applications that generate relevant events and alerts, by integrating data from multiple and different sources. These sources include various types of sensor devices as well as other web resources such as social network feeds, weather data etc.
- ✓ **Scale, Data Volume and Performance -** Managing scale, data volume and velocity is a major challenge that must be addressed in IoT applications. TCUP provides a highly scalable architecture to address the scalability challenge in terms of storage and computation. The implicit need for a secure yet lightweight means to transfer data from sensor devices to cloud, thereby reducing network overload is also supported by the platform.
- ✓ **Flexibility and Evolution of Applications-** In TCUP, sensor configurations and observation data are available as services and are segregated from the applications. Sensor domain data is structured and described using open standards and ontologies. Thus data is self-describing and newer applications can be built by third party application developers easily.

What type of users can be served by TCUP?

[Response]:

- ✓ **Application Developers** will use TCUP for developing and deploying IoT applications. TCUP provides APIs to access services and provides development and deployment support.
- ✓ **Data Scientists** will use TCUP APIs and tools to query, visualize and understand sensor data and conduct experiments on the sensor data using various analytics algorithms.
- ✓ **Administrators** will use the TCUP portal and APIs to create users, create resources and monitor the platform and services health.

What are the types of technologies used within TCUP?

[Response]:

TCUP uses the following technologies to deliver its services –

- ✓ **Web Technologies** – TCUP services are delivered to consumers using web data protocols and standards such as HTTP, XML and JSON. TCUP web portals and web services uses the latest web application frameworks and JavaScript & HTML5 technologies. TCUP provides web application containers as a service to users.
- ✓ **Big Data Technologies** – TCUP provides the ability to store and analyse huge amounts of sensor data by making use of big data and stream processing technologies.
- ✓ **Large Scale Distributed Systems** – TCUP uses scale out and event driven architecture, distributed cache and message queues to provide high scalability, performance and real-time support.
- ✓ **Cloud Computing** – TCUP platform is layered on top of infrastructure cloud services. It uses cloud services to create resources on demand to meet the needs of applications and devices as they scale.
- ✓ **Real-Time Analytical Processing** – TCUP provides the ability to process sensor data streams in real-time using stream processing technologies and rule engines.
- ✓ **Optimized Network Protocols** – TCUP uses low overhead, efficient network protocols for communication between devices and cloud.
- ✓ **Information Modelling** – TCUP provides a common shared sensor data layer. The data layer uses advanced modelling techniques to enable support for virtually any sensor/device and sensor observation. Semantic web technologies are used to enable integration with various other non-sensor data sources.

Why do we call TCUP a platform?

[Response]:

A Platform provides a base to deploy and execute applications. Apart from a set of Web Services with APIs, TCUP provides a multi-tenant application deployment and run time environment. TCUP provides an Application Developers' Portal and the various TCUP services are accessible through this portal. It also provides an Administrator’s Portal which is used by TCUP administrator(s) to perform basic administration task like tenant creation and management, user on boarding, resource provisioning and platform monitoring. TCUP platform runs on top of infrastructure cloud services and provides mechanism for automated installation of TCUP services on computing clusters. Since TCUP provides necessary services for developing, deploying, running, administering and monitoring sensor-driven applications, it is called a platform.

What is a TCUP Application? What is the difference between the TCUP Platform and TCUP Applications?

[Response]:

TCUP Platform consists of horizontal services which can be used for developing, deploying and running sensor-driven IOT applications for any vertical domain like healthcare, transportation, manufacturing, process control, utility, building management etc. By using these services, the application developers can develop domain-specific, big-data enabled, sensor and analytics driven application with relative ease and with reduced time to market. TCUP platform is useful for IOT application developers and infrastructure managers.

The vertical applications which are developed and deployed using the TCUP services are called the TCUP Applications. For example, vehicle tracking can be a TCUP application, or remote patient monitoring can be TCUP Applications as it leverages the horizontal services of the TCUP Platform. In this way any sensor-driven IOT applications can be TCUP Applications. TCUP Applications are useful for users of the applications.

What business problems / use cases can TCUP be applied to?

[Response]:

TCUP can be used to develop and deploy any IoT or M2M applications. These applications can leverage connected devices / sensors and platforms such as TCUP to achieve the following-

- ✓ **Visibility** – Sensors embedded in real world objects (such as personal use devices, assets, equipment, machinery, vehicles etc.) together with data communication capability allow capture of state and context information (observations) in real time and makes it available for further analysis and processing.
- ✓ **Insights** – Aggregation, correlation and fusion of data/observations from different sensors and objects provides unprecedented levels of real-time insights in terms of granularity and breadth. This enables situational awareness at both individual and aggregate level.
- ✓ **Control** – Once insight into state and behaviour of machine-sensors have been obtained, actuators embedded in such machines can be given commands remotely to effect changes in their behaviour and their environment.

Some example of use cases are as follows:-

- ✓ Real-time monitoring of Assets and Machinery for real-time location tracking, condition monitoring, usage tracking, remote diagnostics
- ✓ Connected health and wellness – Remote medical diagnostics and consultation, health and fitness management, chronic disease management and care for the aged
- ✓ Smart Grids, Smart utilities, smart water networks etc.
- ✓ Plant / factory automation
- ✓ Vehicle tracking, telematics, remote diagnostics and servicing of vehicles, driver behaviour monitoring
- ✓ Insurance applications involving remote monitoring of property / home, driving behaviour, prediction of property damage, remote inspection of damages and accidents
- ✓ Intelligent transportation, Fleet tracking and management

What are the key differentiators for TCUP?

[Response]:

TCUP is a comprehensive, standards based, IoT platform aimed at reducing the effort, time and expertise needed to create scalable, secure and robust IoT applications.

- ✓ It is a true cloud and infrastructure agnostic platform, enabling complete freedom with respect to choice of infrastructure or cloud. The use of container technology further allows unprecedented portability across cloud and in-premise infrastructure and enables hybrid operations as well.

- ✓ Built in support for integrating a wide range of IoT devices, gateways, constrained and non-constrained devices and network protocols. Supports ingestion of observations from data files and logs as well.
- ✓ All functionalities are exposed as APIs, enabling developers to create intelligent, end-to-end integrated applications as per business requirements.
- ✓ Support for batch analytics, streaming analytics, rule based processing and data visualization. Support for big data analytics through both batch and stream processing.
- ✓ Data scientists supported by providing runtimes and APIs for analytics job deployment, scheduling and execution using R / Python.
- ✓ An event / message driven, reactive and micro-service based design allows easy extensibility of the platform and integration with external systems, tools and analytics engines.
- ✓ A highly scalable architecture where every layer can be independently scaled in all dimensions to meet any challenging requirements.
- ✓ Uses best of the breed, mature open source components with large community as well as paid subscription support.
- ✓ Various deployment options available – including “In-a-Box” deployments at customer premises, at the edge is also possible.
- ✓ Integrated monitoring and management framework which is essential for smooth operations when applications are deployed in production.

TCUP and Others

How does TCUP compare with other technologies or with the competition?

[Response]:

There are three kinds of players in the market i.e.:-

1) IoT PaaS Providers - by public clouds such as Azure and AWS,
2) Cloud based device management platforms and
3) Niche IoT Platforms.

Each of them have their own limitations and sweet spots.

IoT PaaS Providers

There are various PaaS offerings like Azure IoT, AWS IoT etc., which provide for device data ingestion (primarily via MQTT and http gateways) as well as device registries. These PaaS services can be complemented by other cloud PaaS service offerings such as queueing, stream processing, and server-less computing and big data services.

However these platforms do not provide the necessary support required for modelling and creating application specific needs. They are at a lower level of abstraction and the developer is responsible for modelling and creating IoT application specific schemas, data streams, rules etc.

TCUP services are at a higher level of abstraction than these services. In fact TCUP can leverage these cloud services and can build on top of them. TCUP has a lot of built-in integration so that the developer has to spend less time in stitching together different micro services in order to achieve objective.

A few examples of specialized services provided by TCUP are - Sensor discovery/description/ interfacing/ query/tasking, Sensor Device Management, Event-driven real-time analytics architecture and Sensor specific lightweight communication protocols to reduce communication load on the network.

Cloud-based Sensor and Device Management platforms

There are cloud based sensor platforms for example from Xively, DeviceHive, and Digi which mainly focus on device connectivity, device management and data storage services with very rudimentary support for IoT application development and deployment. Additionally, there is very little support in these platforms for analytics and application management.

Niche IoT Platforms

TCUP is similar in concept to niche IoT platforms such as Predix, ThingWorx, and MindSphere.

Compared to these, TCUP however provides significant flexibility with respect to deployment options, is truly cloud agnostic, does not depend any particular PaaS or cloud stack and is extensible and can be integrated with many third party systems as well as other IoT platforms and IoT clouds.

TCUP micro-services can be used individually, or integrated together, embedded inside other solutions / platforms and can be offered as a white labelled offering as well.

What is the difference between TCUP and a third party IoT platform product?

[Response]:

It must be understood that IoT platforms provide the following major categories of services –

- ✓ Device Management
- ✓ Sensor/Device Data Acquisition and Management
- ✓ Application development and application lifecycle support
- ✓ Support for Telecom Service providers in areas such as – Subscriber Management, SIM Management, and Service Management for M2M etc.

TCUP provides support for the first three categories only. TCUP does not cover the subscriber management, SIM management function etc.

TCUP device management is based on OMA LWM2M standards. For Sensor Data Management – TCUP’s design is influenced by Open Geospatial Consortium Sensor Web Enablement (OGC-SWE) architecture. TCUP has a huge focus on analytics – both Big Data Analytics and real-time analytics and provides data exploration and analytics execution run-time.

A key aspect of TCUP is that it can flexibly be configured as per need and deployed on any public cloud or in-premise data centres. TCUP is also not available as a hosted service.

Is there a specialized instantiation of TCUP on Microsoft Azure cloud?

[Response]:

Yes. TCUP on Azure is a specialized implementation of TCUP that is available on top of Azure Cloud services. It leverages and builds upon Azure Platform-as-a-Service components. TCUP micro-services integrate with and extend Azure IoT services.

TCUP on Azure leverages Azure Virtual Machines for hosting, running and scaling the various TCUP micro-services. It leverages Azure Service Bus and Event Hub as the central messaging back bone between TCUP micro-services and as a repository of real-time event streams respectively. TCUP Message Routing engine works seamlessly on top of these services.

TCUP Sensor Data Management services provides the ability to capture, store, query and analyse data from any type of sensor and manages additional meta-data related to assets, asset properties and locations. It leverages Azure’s big data service, namely Azure HD Insight as the backend data layer. TCUP Sensor Data Management services and Complex Event processing services integrate seamlessly with sensor streams from Azure IoT Hub.

What are the benefits of TCUP on Azure?

[Response]:
Customers using TCUP on Azure get the best of TCUP and Azure PaaS in the following manner–

- ✓ **High system availability and uptime** – Leverages the best of Azure services and deep expertise to achieve very high levels of system availability. This is extremely critical in production environments.

- ✓ **Scalable and Elastic** – The elastic scalability of Azure services means that even as the IoT deployment scales, TCUP on Azure can maintain the expected performance and SLAs vis-à-vis throughput. TCUP architecture follows the best of 3-D scaling approaches and thus can make use of Azure's capabilities.

- ✓ **Cost Effective** – Use of Azure PaaS services considerably reduces both infrastructure costs as well as manpower costs. As highly complex big data platforms and other messaging services are managed by Azure, there is considerably less effort needed in maintaining and administering complex IT systems.

- ✓ **Reduced time to Deployment** – TCUP APIs and the rich collection of Azure services considerably reduce the time from concept to full scale production roll outs

TCUP on Azure is the underlying platform for TCS Building Energy Management solution. This solution has been running in production multiple sites for over a year.

Which verticals can benefit from TCUP?

[Response]:
TCUP is horizontal platform for developing and running sensor-based applications. So it can be useful for any vertical domain in the area of sensor based, M2M (Machine to Machine), IOT (Internet of Things) or Connected-Device applications.

Some examples of such verticals are –

- Telecom – TCUP can be used as a M2M platform by telecom service providers.
- Healthcare – TCUP can be used as a platform for connected health and remote health monitoring applications.
- Manufacturing – TCUP can be used as a platform for remote asset / machinery monitoring and diagnostic applications.
- Automotive – TCUP can be used as a platform for telematics and vehicle tracking applications.
- Transportation – As a platform for fleet management and asset tracking applications.
- Utilities – As a platform for smart grid and energy management applications.

The above list is not exhaustive and TCUP can be useful for many other sensor based applications in similar or other domains.

Deployments

Does TCS run TCUP as a hosted service?

[Response]:

No. TCS can provide a hosted version for evaluation, testing and Proof-of-Concept projects only. For production use, customer has to provide a data centre or cloud subscription for hosting. TCS can provide managed services on these infrastructure as part of a separate contract.

Can we install TCUP within a customer's data centre for his private use?

[Response]:

Yes. TCUP can be installed at customer data centre for their private use. If paid subscription support is required for the necessary open-source components, they needs to be taken into account.

Can we install TCUP in a public cloud?

[Response]:

Yes. TCUP can be installed on public clouds such as AWS, Azure etc. TCUP leverages both IaaS (Infrastructure –as-a-Service) and PaaS (Platform-as-a-Service) components of these clouds. TCUP requires Ubuntu or Red Hat Linux operating system for deployment.

What is the minimum configuration needed for TCUP deployment?

[Response]:

This would depend on what all services are needed. Please discuss with TCUP team for sizing and capacity planning. At a minimum, we recommend 4 physical servers configuration given as:

- 2 Servers (8 Core 32 GB RAM)
- 2 Servers (4 Core 8 GB RAM)

Device Connectivity

How does one interface a device to TCUP?

[Response]:

TCUP provides a library of software modules that makes it easy to connect embedded M2M devices and gateways to the TCUP backend cloud platform. There are two types of connectors provided:-

- ✓ **Device Management Clients/Agents** – These are services run on the device to make it possible for TCUP Device Management Services to connect and manage these devices remotely.
- ✓ **Libraries for ingesting data to TCUP Sensor Data Management** – These are libraries written in C, JavaScript, Python and Java that make it easy to post data to TCUP Sensor Observation Service.

Device Management Clients and Device Connector modules need to be developed for new kinds of devices which are not already supported in TCUP.

What types of devices are supported in TCUP?

[Response]:

Currently the platform includes support for devices/gateways with Android, iOS, ARM/Linux, Arduino and Windows Embedded environments.

What are the networking protocols supported in TCUP?

[Response]:

TCUP continues to enhance support for device integration and network protocol support.

A wide variety of embedded systems, boards and popular IoT device platforms are supported by the platform. Examples of network protocols supported include HTTP(s), MQTT, CoAP, TCP/IP, UDP, LWM2M, OPC UA, MODBUS, Continua and OPC-UA etc.

[Note] Please refer to the TCUP Data sheet for further details

What devices are manageable from TCUP?

[Response]:

Currently TCUP supports the OMA LWM2M standards for device management. So devices with LWM2M compliant device management clients are manageable from TCUP.

What are TCUP Device Connectors?

[Response]:

TCUP provides a library of software modules - termed as Device Connectors - that makes it easy to connect embedded M2M devices and gateways to TCUP backend cloud. Device Connectors are part of application software, deployed on devices or gateways for connecting to TCUP via Sensor Observation Services call. These libraries are written in C, Python and Java that make it easy to post data to TCUP. Device application programmers need to use these libraries in their software code to achieve desired functionality.

What are TCUP Device Management Agents/Clients?

[Response]:

TCUP Device Management Agents/ Clients are running services which execute on the device to make it possible for TCUP Device Management Services to connect and manage these devices remotely. The Device Management Agent/Client enable devices to connect to TCUP Device Management server and vice versa. The Device Management server can send data updates and commands to devices using the device management protocol. Also, the server can "observe" the state of the device and sensor values and can automatically detect any changes in observed parameters. These changes are transmitted to the device management server using device management protocol. The device management server in turn can post the data to TCUP Sensor Observation Service.

The fundamental difference in the Device Connector approach versus the Device Management Agent/ Client approach is that in the former the device side application must be compiled with TCUP connector libraries, whereas in the latter, no custom application needs to be written. For supported devices, a client software has to be deployed instead. Also in the latter, no APIs call is needed from device end.

How do I send sensor observations from a device to TCUP using the Sensor Observation Service (SOS)?

[Response]:

Sensor observations are sent to SOS via API calls. These APIs are RESTful and use either http(s) or CoAP protocols. You can use TCUP connector libraries for the same. Observation data in JSON (Java Script Object Notation) format is sent as payload in the API calls. API keys allocated to the user needs to passed in the request header of the REST API as well.

I have a device X – how can I integrate it with TCUP Sensor Observation Service?

[Response]:

If we can deploy and run custom application software on the device X and if the device supports a TCP/IP stack (including HTTP / CoAP / MQTT client), we can connect it via API calls. We need to develop a custom application that includes the connector library and deploy the code on the device.

If the device is not programmable or if we cannot deploy an application on the device or the network connectivity with TCP/IP support is not available, then we need to write a custom software to interface with device X and execute the same on an edge-gateway device. The gateway needs to have HTTP/COAP / MQTT support in that case. The device connect to the gateway via short-range communication protocol like Wi-Fi, Bluetooth, ZigBee or wired connection and data is transferred over this connection from the device to the gateway. Data is transferred from gateway to TCUP Cloud via RESTful TCUP SOS (Sensor Observation Service) API.

I have a device Y – how can I manage it with TCUP device management?

[Response]:

If the device Y is of a type for which TCUP Device Management Agent/Client exists, then the device can be managed by TCUP Device Management Server.

Analytics

What types of analytics is possible on TCUP?

[Response]:

TCUP Analytics services can be classified into 2 categories:

1. Batch Analytics (Via Task Service APIs)
2. Real Time Analytics (Via Message Router and Complex Event Processing Service APIs)

Batch Analytics

Batch data processing and analysis involves processing high volumes of data collected over a period of time and performing analysis on this data in batch mode.

TCUP enables a large number of batch programs running analytics workloads to be executed in parallel on large server clusters. Developers can configure the platform by providing the path to the program and specifying the path to the data (on which the program will execute). TCUP is able to execute these programs (typically written in languages such as R or Python) on behalf of the user at scheduled or on-demand basis on available servers in the cluster and return the output results.

Real time Analytics

TCUP provides following two types of real time analytics:

- ✓ Message Routing and Filtering – This involves rule based selection, filtering, grouping and routing of event streams. Geo fencing and event enrichment is also supported.
- ✓ Complex Event Processing- This involves analysing multiple sequences of streaming data, such as aggregation, correlation, condition based filtering, etc.

What tools support does TCUP provide for analytics on sensor data?

[Response]:

TCUP provides search, reporting, dashboards and charting facilities. These are supported via Elastic Search.

TCUP Sensor Observation Service data is available on Apache HBase and these can be processed using tools from the Hadoop family. TCUP data can also be loaded on to Apache Spark.

TCUP Task Services allows programs written in R or Python to be executed at scale. All analytics packages available on R and Python can therefore be used to operate on TCUP.

Does TCUP provide any out of the box algorithms for a particular domain?

[Response]:

No. Any domain or application specific analytics has to be developed separately by the application development team.

Applications

What type of API does TCUP support?

[Response]:
TCUP provides REST APIs for all its services. These APIs can be called from any language or runtime. These APIs use JSON as the message payload.

What are the applications servers/frameworks supported for web applications deployment on TCUP?

[Response]:
TCUP supports web applications on Apache Tomcat and Play Framework.

What are the programming languages for batch programs on TCUP?

[Response]:
TCUP Task Services can run batch programs written in R, Python, Java and C.

I have an existing application – how do I interface it with TCUP?

[Response]:
Applications can interface with TCUP via REST API calls. Application need an API key to call APIs.
For accessing TCUP portal User Id and Password is required.

I have an existing .NET application – can I run it on TCUP platform?

[Response]:
TCUP does not provide a .NET runtime. However, .NET applications can call TCUP APIs.

We are conceptualizing a PoC (Proof of Concept) M2M application for a potential customer. But we do not have access to real sensors as of now. Can TCUP help us?

[Response]:

Yes. TCUP has a utility to simulate sensors and observation and measurements from sensors. You can start developing the application using the simulated sensors. Later on when you have access to the real sensors, you can interface them with the rest of your application.

Security

How does the platform handle security? How is Security handled from devices to platform?

[Response]:

Security for the platform is at 3 levels i.e.

- ✓ Endpoint security,
- ✓ Platform security and
- ✓ Communication security.

Endpoint Security

How does TCUP ensure endpoint authentication?

[Response]:

In TCS Connected Universe Platform, all devices communicating with cloud based services have to authenticate themselves by presenting certificates and digitally signing their messages. The servers authenticate the certificates presented and verify the signatures.

What kind of hardening is necessary for TCUP endpoints?

[Response]:

TCUP endpoint hardening consists of running a minimal OS image, with all unnecessary services stopped and all non-required network ports disabled. TCUP device agents would run with minimal privileges.

What is Secure Bootstrapping?

[Response]:

Secure bootstrapping allows a device to securely discover a device management server and get necessary credentials to register itself. TCUP Device Agent/ Clients connects to the Bootstrap Server using pre-shared secret keys using a secure channel (TLS/DTLS) and receives necessary credentials and paths to the Device Management Server. The Device Management Server and the Device Management Agent/Client mutually authenticate each other using the pre-shared keys.

Does TCUP provide Secure Over-The-Air (OTA) Provisioning?

[Response]:

TCUP provides secure OTA. Over-The-Air (OTA) upgrade is done over secured channel (using TLS) by mutual authentication using asymmetric key encryption. The devices validates any upgrade package received from server for its integrity, decrypts the same using server's public key prior to installation.

Communication Security

How does TCUP ensure server authentication?

[Response]:

TCUP clients should ensure that they communicate to only trusted servers. This is ensured in the TLS / DTLS sessions when the server presents its certificates to the client devices. The clients verify the servers' certificates by authenticating them against root certificates stored within the client devices. TCUP can make use of PKI to issue, manage and revoke certificates for servers and devices/clients.

How does TCUP ensure network security?

[Response]:

TCUP device connectors and device agents use standard TLS or DTLS protocols for network security. TLS is used when transport in TCP/IP and DTLS when transport is UDP/IP.

What are additional communication security mechanisms used in TCUP?

[Response]:

VPN (Virtual Private Network) - Additional ways of reducing attack surface involves use of a VPN to create private overlay networks on top of public internet. This would ensure that the entire IoT network is visible only to trusted sites and endpoints that have been configured with the VPN clients.

HSTS (HTTP Strict Transport Security) has been implemented which forces the client (web browsers) to communicate with servers over HTTPS only. At server end, request re-direction has been implemented to translate any incoming HTTP requests to HTTPS.

Platform Security

What does the TCUP API Gateway do?

[Response]:

API Gateway is used for providing a security layer and rate limiting to any TCS Connected Universe Platform service access. All service calls hit the Gateway first, where the API caller is authenticated and it is also checked if the particular service call has been enabled for that caller. A fine-grained access control mechanism can be enabled using TCS Connected Universe Platform API Gateway.

Additionally, the API Gateway checks if the rate limits associated with that caller has been exceeded or not. If limit have been exceeded, then all subsequent calls are blocked. This is quite a useful feature in dealing with Denial –of-Service (DoS) attacks by limiting the exposure of the service to the Gateway itself. Further, rogue client access can be further prevented by blacklisting certain IP addresses or by white listing only certain network addresses.

What are the different API security measures used in TCUP?

[Response]:

API authentication is done using a combination of API keys and authorization tokens.

API Keys are a set of public identities and secrets that are issued for each TCS Connected Universe Platform tenant/developer. The API Key (identity) must be passed in the HTTP(s) header of each API call. This key is used to validate the client.

Additionally, it is possible to create key-based cryptographic message digests (HMAC) for the payload in each API call and pass as a header of each API call. These digests are verified in the server end since the secrets are shared and known to both end points (secret key never gets transmitted for API calls). Access is given to a particular API call only after validating the digest/signature at both ends.

JSON Web Token (JWT) based authentication may also be used as an additional security measure for API access.

What are various Security testing/scanning processes that TCUP platform goes through?

[Response]:

TCUP goes through various security testing and validation phases prior to release:-‘

- ✓ **SAST (Static Application Security Test)** – This is performed by TCS Enterprise Security & Risk Management (ESRM) team to analyse application source code for any potential vulnerability and also highlights violation of standard coding practices and guidelines. Tools used include HP Fortify.

- ✓ **DAST (Dynamic Application Security Testing)** – This is performed by specialized security team from ESRM to check application vulnerabilities as per OWASP guidelines. Tools used include HP Web Inspect, Burpsuite, Sqlmap, Wireshark etc.

- ✓ **VAPT (Vulnerability Assessment and Penetration Test)** – This is again performed by the specialized security team from ESRM to test network level vulnerability. Tools used include NMap, Nessus Pro, Metasploit Framework, Fuzzing Tools, Manual Scripts etc.