TruU Security Whitepaper

TruU Security Whitepaper
Version 6.1
March, 2021

TruU, Inc.
720 University Ave., Suite 200
Palo Alto, CA 94301
United States

Website: https://www.truu.ai

Trademark

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. TruU, Inc. does not provide any warranties and specifically disclaims any liability in connection with this document.

Table of Contents

Introduction 4

TruU Platform Architecture 5

TruU Component Overview 6

FIDO Registration Flow Using Biometrics 7

FIDO Authentication Flow Using Biometrics 8

Authentication for Workstation Full Domain Login 9

Data Privacy 11

Enterprise Data 11

User Mobile Metadata 11

User Mobile Metadata Transfer 12

Heartbeat Transfer and Storage 12

TruU Identity Platform Availability 13

Application Delivery 13

Database Availability and Security 13

Data Storage and Backups 14

Identity Platform Recovery 14

Identity Platform Security 14

TruU Identity Platform 14

TruU Identity Server 14

Enrollment API 15

Identity API 15

TruU Management Server 15

TruU Management Server Administrative Account 15

AWS Key Storage 15

Multi-tenancy 16

Securing Communication with OAuth 2.0 17

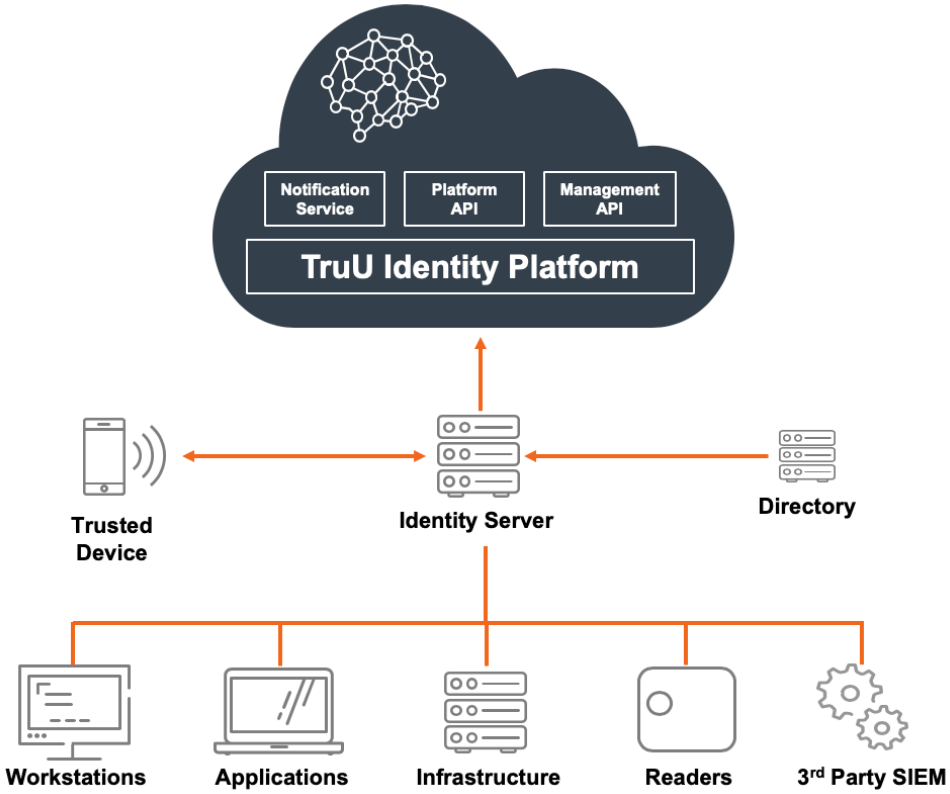
Conclusion 17

Introduction

With any security solution, the provider must be trusted to protect an Enterprise's most valuable resources. As an identity management solution provider, TruU understands the importance of the functionality it provides and places security as a top priority.

This document describes the components of the TruU solution and its design for security, privacy, data protection and availability. These technologies are coupled with a company-wide commitment to security, operational excellence and respect for customer data. We take your identity and privacy as seriously as we take our own at TruU.

TruU Platform Architecture



- **TruU Identity Platform** is a Software-as-a-Service offering that enables password-less multifactor authentication to digital resources and badge-less multifactor access to physical resources. The Identity Platform provides a Management Console for Administrators to configure policies, download adapters and monitor their overall environment.

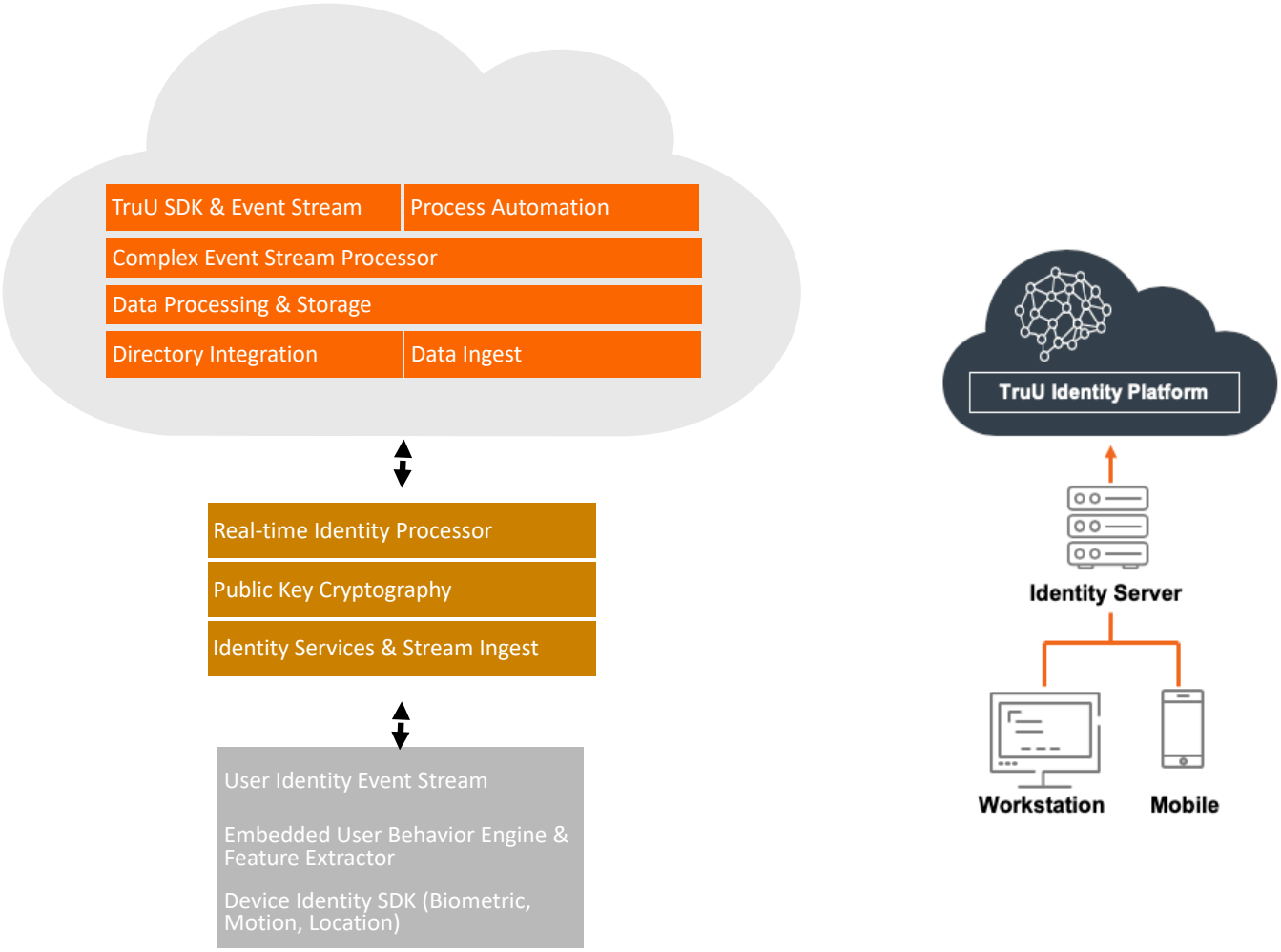
- **TruU Identity Server** can be hosted by TruU or can be deployed as customer managed software that can run as a service on a host server or within a Docker Container. The Identity Server provides a range of capabilities that includes determining the identity of a user, device registration, PKI management, FIDO authentication and more. Identity Servers communicate with the TruU Identity Platform, User Directory and resources through TruU Adapters. Identity Servers are deployable in a cluster for high availability, fault tolerance and redundancy.

- **TruU Adapters & Agents** enables TruU to provide access decisions to a variety of resources that include workstations, Identity-as-a-Service (IDaaS) for applications, infrastructure (servers & network devices), physical access control systems (PACS) and more.

- **TruU Mobile App** enables access to TruU enabled resources. The TruU mobile app is available in the public app stores for both iOS and Android platforms.

TruU Component Overview

The following diagram illustrates the various services and software components that collectively make-up the TruU Platform. The core components consist of the TruU Identity Platform (cloud) and TruU Identity Servers. The Identity Platform is configurable (if enabled by an Administrator and permitted by User) to ingest sensor data from registered devices through the TruU mobile app/agent. The Identity Platform performs most of the data processing using machine learning and artificial intelligence algorithms to verify a User. Identity Servers communicate with the Identity Platform in order to retrieve behavioral models and policy configurations needed for Identity Servers to make authentication decisions for a User. The Identity Server also provides a variety of services including serving as a FIDO authenticator, PKI management, device registration and more.



TruU Registration and Authentication

The TruU Mobile App binds the user's mobile device to the user through a registration process. Once registered, the TruU Mobile App enables the user to prove their identity through biometric and/or behavior identification of the user.

FIDO Registration Flow Using Biometrics

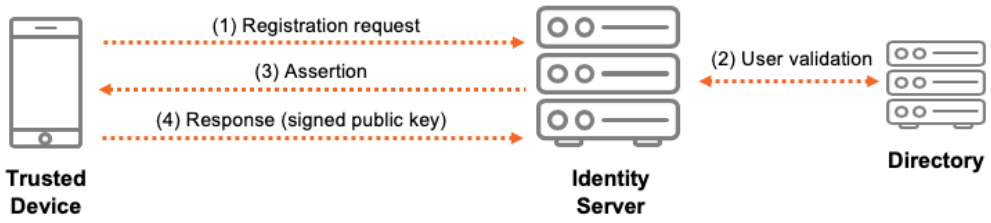
TruU leverages a FIDO Universal Authentication Framework (UAF) flow with biometrics for secure registration of a User's device with the TruU service. A User's TruU identity is established through validation against an Enterprise's LDAP directory and a biometric challenge on the User's mobile device. The registration flow is as follows:

1) A User initiates a registration request to the TruU service (the Organization's TruU Identity Server) via the TruU mobile app.

2) The Identity Server validates the User's identity and status (e.g. active/inactive) in the Organization's user directory.

3) The Identity Server presents a registration assertion to the User upon which the User is prompted for biometrics. If biometrics of the registering User match biometrics setup on the device, a public/private key pair is generated on the device. The private key signs the registration assertion for the User, then is stored in the device's secure storage.

4) The signed registration assertion and the User's public key are returned to the Identity Server – completing the registration flow.



FIDO Authentication Flow Using Biometrics

TruU leverages a FIDO Universal Authentication Framework (UAF) flow with biometrics to validate the identity of a User before granting access to TruU enabled resource. The authentication flow is as follows:

1) A User initiates an authentication request to a TruU enabled resource.

2) The resource publishes an authentication request with the TruU Identity Server, for which the Identity Server will validate the User's identity using a FIDO authentication flow.

3) The Identity Server validates the User's status (e.g. active/inactive) in directory and validates policies configured within the TruU Management Console.

4) The Identity Server sends an identity request to the User's device via a push notification.

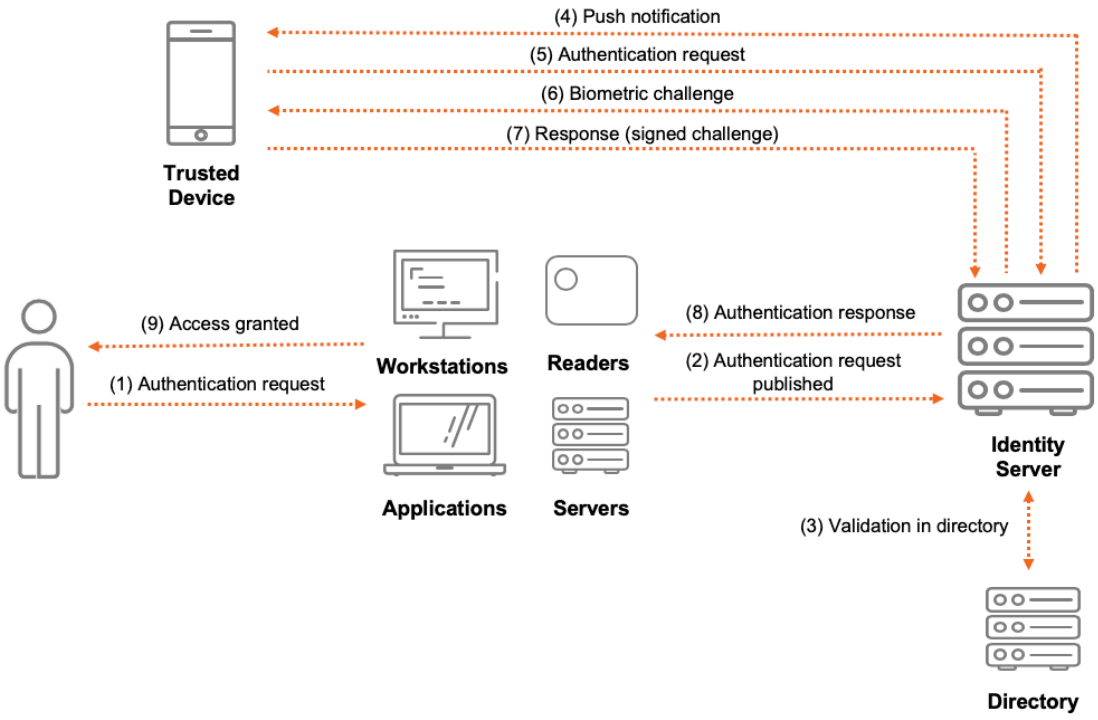
5) The User responds to the identity request by providing intent for access.

6) The Identity Server presents a biometric challenge for the User to validate identity.

7) The User provides biometrics to confirm identity. The response is signed by the User's private key (generated during device enrollment) and sent back to the Identity Server.

8) The Identity Server provides an authentication response to the resource (identity is valid).

9) The User is granted access to the resource.



Authentication for Workstation Full Domain Login

TruU leverages a FIDO-like flow with validation and policy enforcement to issue a signed certificate for a corresponding private key (a PIV card certificate under the covers) generated on and tethered to the secure enclave of the mobile device for workstation login. These “PIV cards” are used with the workstation agent either over a network connection or Bluetooth low energy. https://en.wikipedia.org/wiki/FIPS_201. The use, life cycle, and revocation of these PIV card certificates are automated without the use of classic (and commonly painful) plastic smart cards.

PIV card transactions for workstation login and unlock are one-time challenges with cryptographic signing of the single use random data. Thus, even if it were observed in the clear, it is not possible to replay and there is nothing personal or secret.

However, to keep even those transaction private and ensure a high level of trust and integrity, TruU adds additional layers of communication protection. First, all communication via network is secured via TLS, including the initial establishment of the pairing between the TruU mobile app and TruU desktop service used for subsequent network and Bluetooth LE transactions.

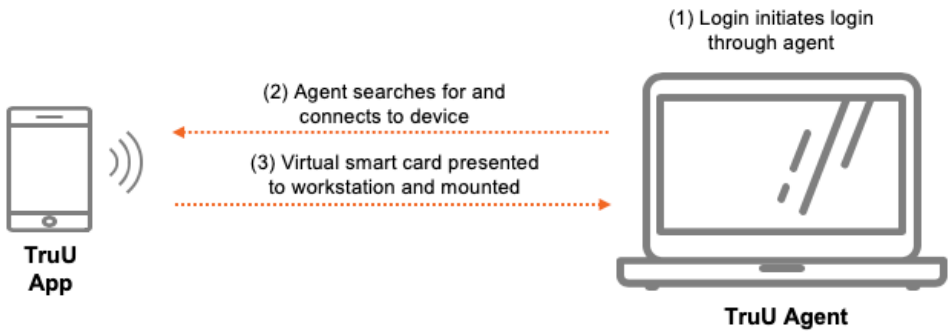
Next, although native Bluetooth LE pairing between mobile device and desktop operating system offers only AES 128bit protection per the specification, TruU believes the cryptography should be stronger than that. Therefore, with Bluetooth LE, TruU uses a BLE Generic Attribute Profile (GATT) communication where the transport over the air is considered completely untrusted. The TruU desktop service and mobile agent use asymmetric public/private keys based on initial trust first established when the TruU mobile app is paired with the TruU desktop service allowing for AES 256bit (or greater in the future). These asymmetric keys are currently dynamically generated and rotated on every full login.

The Bluetooth LE authentication flow is as follows:

1) User initiates a login request through the TruU desktop agent.

2) The desktop agent searches for a known and paired TruU mobile app and establishes a Bluetooth LE connection to the app. If this is a full logon, new asymmetric keys are dynamically generated and securely exchanged leveraging the existing trust. If this is a workstation unlock, then the existing keys will be used. Once established a randomized one-time challenge communication will take place from the workstation TruU service to mobile device.

3) The desktop agent mounts a virtual smart card to the operating system for login; however, all workstation communication is routed through the TruU service to the TruU mobile app’s PIV card. TruU mobile app uses the PIV card to sign the challenge and return it to the desktop agent.



In addition, TruU's workstation offering includes various proximity capabilities. To protect against Bluetooth LE cloning of advertised services, the TruU service on the workstation will challenge the TruU mobile app directly via a transaction that can only be answered by the real paired app. That transaction cannot be replayed.

The Network authentication flow is similar to the Bluetooth LE communication flow; however, the network communication is encrypted via TLS.

Lastly, a typical pairing of the TruU mobile app to the workstation's TruU service (desktop agent) is achieved on a first-time login by scanning the QR code presented by the workstation's TruU credential provider. Upon scanning the QR, the TruU mobile app establishes the network connection, pairs the TruU mobile app with the workstation TruU service, authenticates the user, and processes the workstation login challenge. That pairing between the TruU mobile app and workstation TruU service is the same pairing that is used by TruU Bluetooth LE transactions.

In Summary:

a) Even with no transport encryption – the communication is of a randomized, reply-safe, cryptographic challenge and cannot be re-used to login more than that one time to that one single workstation.
b) The PIV based certificates are tethered to the secure hardware and never leave the mobile device. The use, life cycle, and revocation of these PIV card certificates are automated without the use of classic (and commonly painful) plastic smart cards.
c) For Bluetooth Low Energy, we don't trust the "weak" native encryption from the specification. Instead, we treat the transport as untrusted and use strong encryption based on asymmetric keys that are dynamically generated and rotated upon each full login.
d) Network communication is always encrypted via TLS.

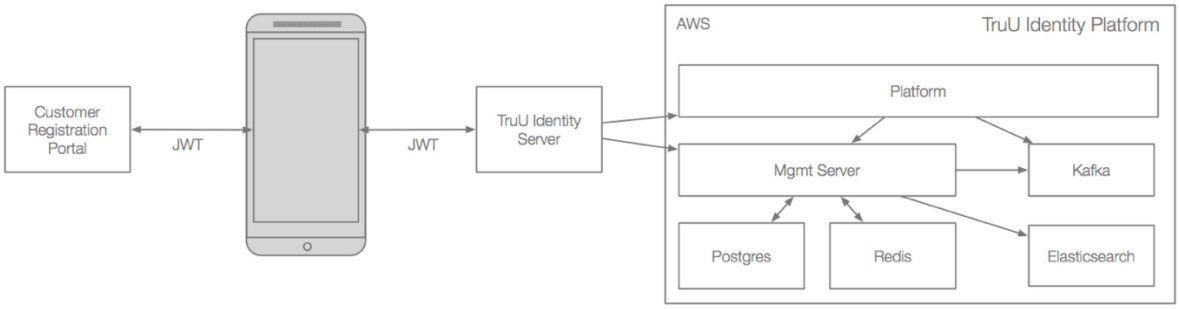
Data Privacy

TruU takes data and user privacy very seriously and all data is carefully protected.

Enterprise Data

Enterprise data is defined as data created, owned and managed by the Enterprise. Enterprise systems that retain this data include an HR application or a user directory. The TruU Identity Server integrates with an Enterprise's directory (Active Directory, Azure Active Directory, External Datastore, Okta) to authenticate a user using biometric or behavior in place of a password. Communication between the TruU Identity Server and directory and storage of the directory credentials within the TruU Identity Platform are secured by the following:

- Read-only credentials to directory are required by TruU to query users in directory. These credentials are set in a Customer's tenant (on the TruU Identity Platform), encrypted and stored in a PostgresSQL database. Encryption keys are stored in AWS Key Management Service (KMS).
- Enterprise data stored: GUID, DisplayName, UserPrincipalName, Email.



User Mobile Metadata

Basic metadata from a registered mobile device is captured and retained in the TruU Identity Platform. This information provides a System Administrator with visibility into the devices that are registered to a particular user and the hardware and software versions of those devices for security purposes. TruU captures the following metadata during device registration:

- **DeviceID:** A unique alphanumeric string generated by TruU to identify a device.
- **Time Stamp**: Unix time stamp.
- **Time Zone:** The time zone the mobile device is configured with.
- **Hardware Version:** The hardware version of the mobile device.
- **Software Version:** The version of the TruU mobile app or SDK.

User Mobile Metadata Transfer

Devices communicate with the TruU Identity Server for registration and authentication events. Device metadata is securely transferred and stored by the following:

- All data at rest is secured with AES-256-bit encryption.
- All data in motion is secured with TLS1.2 or higher.
- Access to the AWS VPC is limited and secured with TruU authentication.

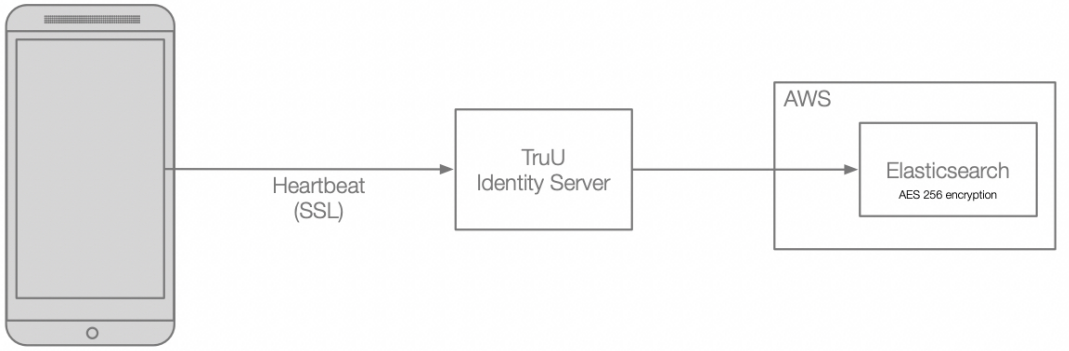
Heartbeat Transfer and Storage

The device Heartbeat Service enables TruU to periodically check the connection status between a registered device and the TruU Identity Platform. Heartbeats also enable the TruU app or SDK to communicate with the appropriate Identity Server(s) and provides TruU with diagnostic data required for operation. The following metadata is sent from a device to TruU in a heartbeat:

- **Device ID:** A unique alphanumeric string generated by TruU to identify a device.
- **Software Version:** The version of the TruU app.
- **SDK Version:** The version of the TruU SDK.
- **OS Version:** The version of the device's operating system.
- **TUID:** An alphanumeric string that uniquely identifies a user to TruU.
- **Display Name:** The Active Directory display name of a user.
- **Domain ID:** The TruU tenant a user is registered to.
- **Total Disk Space:** The total amount of disk space on the device.
- **Remaining Disk Space:** The amount of disk space remaining on the device.
- **Used Disk Space:** The amount of disk space used on the device.
- **Successful Uploads:** The number of successful data uploads made between the device and the TruU Identity Platform.
- **Failed Uploads:** The number of failed data upload attempts made between the device and the TruU Identity Platform.
- **Last Launched:** The last time the TruU app or SDK was initially launched on the device.
- **Last Opened:** The last time the TruU app or SDK was last opened on the device.
- **Battery:** The amount of battery remaining and battery health.

Heartbeat messages are securely transferred from a mobile device and stored in the TruU Identity Platform by the following:

- All data at rest is secured with AES-256-bit encryption.
- All data in motion is secured with TLS1.2 or greater.
- Access to the AWS VPC is limited and secured with TruU authentication.



TruU Identity Platform Availability

The TruU Identity Platform is deployed across multiple Amazon Web Services (AWS) regions and availability zones. AWS data center reliability is foundational to the availability of the TruU Identity Platform.

Application Delivery

TruU achieves a high degree of availability and security by integrating its technology stack with AWS cloud service infrastructure and enterprise automation tools.

Customers interface with the TruU Identity Platform through AWS Application Load Balancers. These load balancers are deployed to multiple availability zones, automatically scale based on demand, and enforce TLS 1.2 for network security.

The applications underpinning the TruU Identity Platform are deployed on the Amazon Elastic Container Service (ECS). ECS provides autonomous orchestration, supporting on-demand scaling and seamless upgrades. Enterprise automation tools reduce availability risk when the TruU Identity Platform upgrades are deployed during change windows.

Database Availability and Security

TruU uses the Amazon Relational Database Service (RDS) to support the Identity Platform. TruU RDS instances span multiple data center availability zones. Daily snapshots and full weekly backups support durability. Furthermore, RDS instances are configured to use encryption at rest and in transit.

Data Storage and Backups

TruU relies on the AWS Simple Storage Service (S3) for three distinct use cases:

- Storing static web content for the TruU management server
- Storing Identity Server and Adapter download files that are accessed from the TruU Management Server

AWS promises extreme data durability with S3, and TruU supplements this by archiving daily snapshots of critical buckets to S3 Glacier. TruU S3 buckets are configured to use encryption at rest.

Identity Platform Recovery

TruU has established backup protocols to ensure data survivability. TruU engineers have compiled a Recovery Runbook to document data and system recovery procedures from these backups. Automation--currently used to deploy updates to the TruU Identity Platform--will be leveraged for these Runbook procedures wherever possible to ensure timely and reliable recovery operations.

Identity Platform Security

TruU Identity Platform API endpoints are tightly controlled, using OAuth 2.0 for authentication and authorization. Only enrolled clients (i.e., TruU Mobile App or SDK users) can access Identity endpoints. Similarly, only authenticated administrators or provisioned API clients can access Management endpoints. Using OAuth 2.0, the TruU Identity Platform limits the scope of actions that an authenticated client can exercise.

TruU Identity Platform

The TruU Identity Platform relies on a message routing service simply referred to as the Platform. The Platform serves as a communication conduit between TruU Identity Servers (often deployed in customer data centers) and the TruU data processing services deployed in the TruU cloud. Importantly, the Platform serves as the TruU OAuth 2.0 authorization server. Clients (including the TruU Mobile App/SDK, Identity Servers, Management Server, and data processing services) all rely on the TruU Platform for the granting of OAuth tokens commensurate with their access needs (i.e. a client's scope). TruU Identity Platform API endpoints act as OAuth resource servers, validating OAuth tokens presented by clients.

TruU Identity Server

The confidentiality of all communication with TruU Identity Servers is protected using TLS 1.2. Authentication and authorization to Identity Server API endpoints is secured with OAuth 2.0.

Enrollment API

New clients (i.e. mobile device with TruU mobile app, workstations with TruU desktop agent, servers with TruU PAM adapter) bootstrap trust within the TruU Identity Platform through a FIDO enrollment process with a TruU Identity Server. Once enrolled, clients request OAuth tokens from the TruU Platform in order to access TruU Identity APIs.

Identity API

Post-enrollment transactions between a client and TruU Identity Server require presentation of a valid OAuth token. Examples include the biometric fulfillment of identity requests via the FIDO protocol, requests to unlock doors, and periodic health and status messages ("heartbeats") sent by the TruU Mobile App.

TruU Management Server

The TruU Management Console is the administrative interface for deploying TruU. The Management Console is API-based: all actions within the user interface translate to RESTful API calls to the Management Console web application. All Management Console API endpoints require that a valid OAuth token be presented. The Management Console web interface transparently passes OAuth tokens to the back-end API on behalf of an authenticated administrator.

Similarly, TruU Identity Servers present valid OAuth tokens when communicating with the TruU Management Console (refer to '**Securing Communication with OAuth 2.0**' section).

TruU Management Server Administrative Account

A customer can maintain one (and only one) username and password-enabled administrative account to their TruU Management Console. This administrative account can create additional administrative users, but these users can only authenticate to the TruU Management Console via SAML. Once SAML login is enabled, login with username/password can be disabled to the TruU Management Console. Administrative provisioning in this manner supports role-based access control to the TruU Management Console.

AWS Key Storage

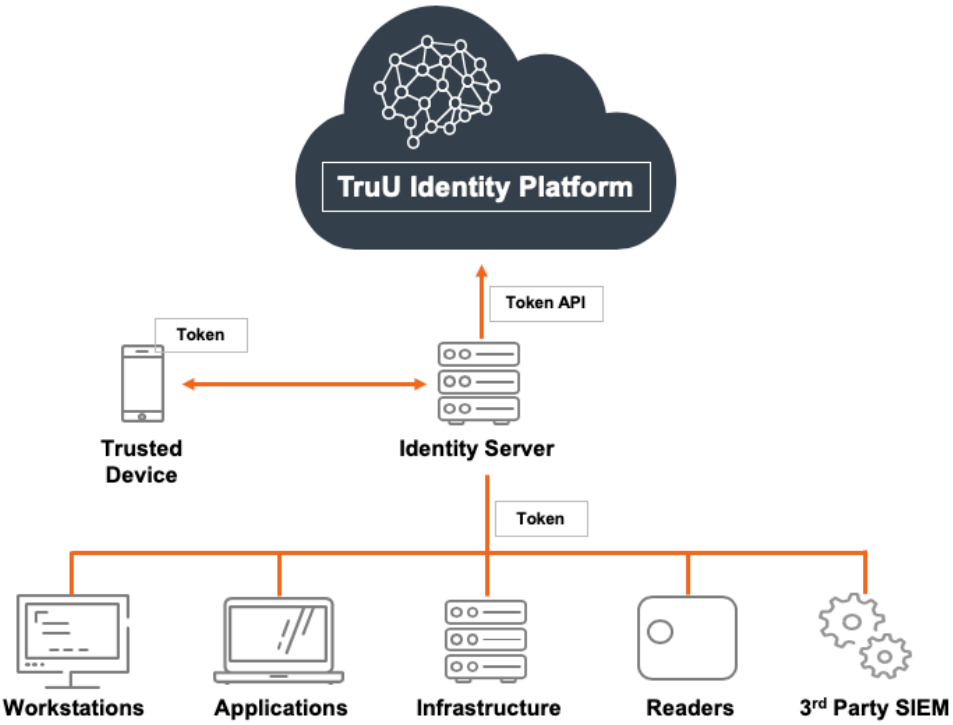
TruU uses Amazon's Key Management System (KMS) to maintain keys. The AWS KMS is a managed service that enables Enterprises to create and control keys used to encrypt their data. The AWS KMS is designed so that no one, including AWS employees, can retrieve the plaintext keys from the service. The service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of the keys. Plaintext keys are never written to disk and only ever used in volatile memory of the HSMs for the time needed to perform a requested cryptographic operation. Keys stored within a KMS are never transmitted outside of the AWS region in which they were created. Updates to the KMS HSM firmware are controlled by multi-party access controls that are audited and reviewed by an independent group within Amazon. AWS HSMs are also compliant with a number of security certifications, which include HIPPA, SOC 1, SOC 2 and SOC 3.

For more information about AWS HSMs, refer to the following AWS whitepaper:
https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

Multi-tenancy

The TruU Identity Platform is a single Software-as-a-Service instance built and hosted on AWS. The TruU Identity Platform is responsible for ingesting sensor data from registered devices and processing the data using machine learning and artificial intelligence algorithms. Each TruU customer is provided with their own TruU Identity Platform tenant, which allows System Administrators to manage registered devices, configure registration and authentication policies and view event data such as login details of a user (e.g. name of application the user logged into, if biometric or behavior was used for login and if the authentication event was successful). To protect each customer's data within the TruU Identity Platform, TruU generates a unique domainID that is associated to one and only one customer tenant. The domainID is included as part of the primary key in every database record, which enables a customer to only access data within their own tenant. While data processing is performed in TruU's Identity Platform, all identity and authentication decisions are performed by TruU Identity Servers. Identity Servers are single tenant instances deployed and managed by the customer. TruU Identity Servers securely communicate with the TruU Identity Platform for policy updates using a unique security token generated within a customer's tenant. This ensures that each TruU Identity Server only communicates with the appropriate tenant.

Securing Communication with OAuth 2.0



TruU secures communication between mobile devices, workstations, Identity Servers and adapters with OAuth scopes and authorization tokens. The TruU Identity Platform functions as an authorization server that issues OAuth tokens to TruU clients. Clients include mobile devices with the TruU app/SDK, workstations with TruU agent, Identity Servers and TruU Adapters. When a client, such as a mobile device, communicates with a resource, such as an Identity Server, an OAuth token is issued to the client by the TruU Identity Platform and validated by the resource. If the OAuth token is valid, the resource will authorize access to the client and restrict access based on a defined OAuth scope. The client identifier and secret, used to request OAuth tokens, are securely generated and communicated to the TruU Identity Platform during mobile device enrollment. The client identifiers and secrets assigned to Identity Servers and Adapters are securely generated and issued when deployed through the TruU Management Console.

Conclusion

TruU is committed to protecting customer data and ensuring security, confidentiality, privacy, integrity and availability of its offering. From its hiring practices to the software it develops and the operational environment in which it runs on, TruU understands the importance of protecting its customers and maintaining a highly available solution. For more information, please contact TruU at https://www.truu.ai/contact-us.