An TipTop Platform White Paper 2021

TipTop Platform IAM solutions for Application, Users, Employee , Customer , Devices and Business Users with advanced 5th generation Identity and Access Management

Websites

www.tiptopplanet.com
www.ahalspay.com www.ahals.com
www.hrsep.com

Tiptop Platform IAM Platform

TipTop Platform Identity and Access Management systems and services provide new technical capabilities for organizations to unify their entire identity and access management requirement may it be Applications or Physical access using IOT devices . Implementing TipTop Identity’s solutions for IAM can provide Secured and Robust IAM environment with better user experiences and integrated Multidimensional organization chart and AHALTS validation with advanced Biometrics that include Face recognition and finger Print validation beside conventional multifactor Authentication services. The system gives a ready organizational IT unification framework with Lowest cost of ownership.

Table of Contents

1Executive Summary

Unified IAM for Application, Devices , Employee And Customer Identity and Access Management (IAM) is the fastest growing specialty in Identity and Access Management(IAM)that has emerged in the last few years to meet evolving business requirements especially after IIOT revolution as the future IAM has to be Device and Application ready as lots of M2M (Machine to Machine a) and A2A (Application to Application) have started interacting to each other with Robots and Bots increasing day by day.

Many businesses and public sector organizations are finding that they must provide better digital experiences for and gather more information about the Employees or users who are using their services. Enterprises want to collect, store, and analyze data on Employees and Consumers to create Great Employee experience and reduction in HR and IT department workloads in addition to sales opportunities and increase brand loyalty.
For example, to reduce Proxy Identities in case of Employees or money laundering, cyber-crime, terrorist financing, and fraud, regulators are requiring banks and financial service providers to put into place mechanisms for "Knowing Your Employee And Customer" (KYC). Having IAM systems dedicated to hosting User identities and their associatedprofiles is a necessary first step toward KYC.

Employee And Customer Identity solutions

- Provide self-registration for Employee And Customers
- Alternatively, provide options for bulk import of Employee And Customer identities from existing systems
- Give users consent mechanisms to control the use of their data
- Enable Single Sign-On(SSO)across all digital properties
- Present multiple authentications options for Employee And Customers, depending on policies, risks, and mechanisms available
- Manage unified Employee And Customer profiles
- Facilitate fine-grained access control to resources and data
- Application and Device Identity solutions
- Application can be registered for developers giving them a access to other application Resources and also give a application level access control based on licensing and user permission options
- Device can be registered for M2M communication so that Devices can interact with users , applications etc.

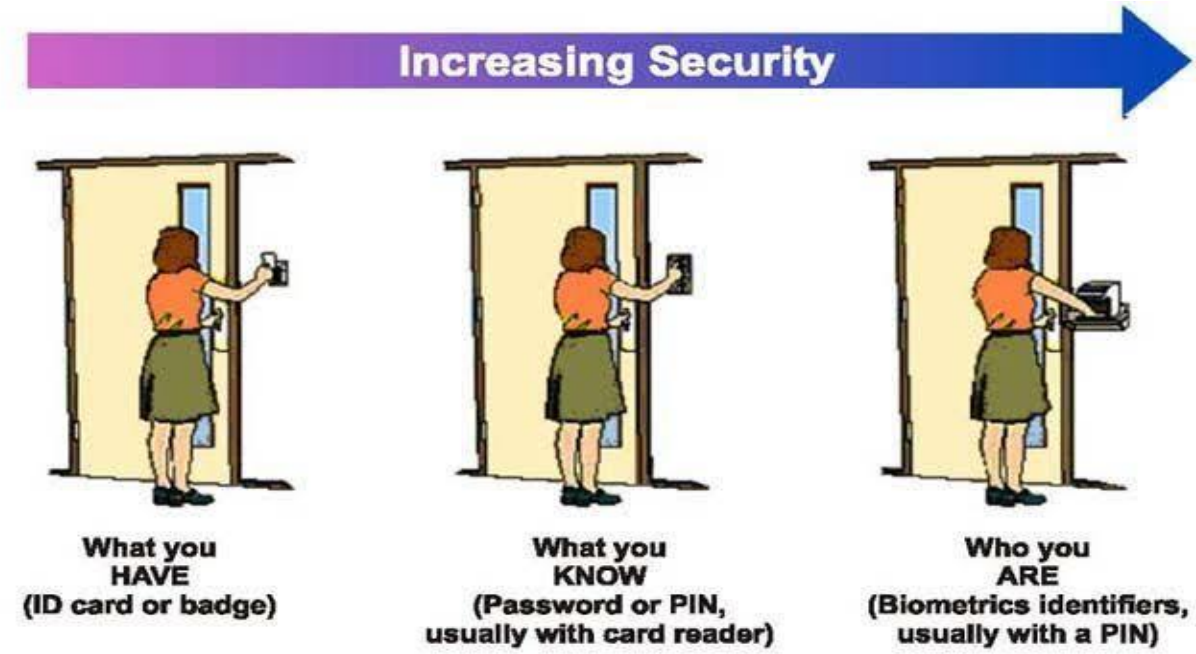
Delivery Model

- Can be deployed on-premise, in the cloud or both
- Scale to support millions of Employees and Consumers, peak usage scenarios, and ensure performance and availability SLAs are met.

This paper explores IAM concepts, business drivers, challenges of designing IAM solutions, and the entry points into solution architectures. The paper will further show how Tip Top Platform products can help meet both the business requirements and challenges of Application, Devices , Employee And Customer identity by providing a robust, scalable, and future-embracing solution set.

2 Highlights

- Creating a Central Identity and Access control framework so that the entire It and physical assets can be given Identity and also their access can be controlled from a central repository
- Employee And Customers want a pleasant, consistent digital experience when interacting with brands across all channels and devices.
- Employee And Customers do not tolerate painful site registration processes, difficult authentication, or slow system response times. Employee And Customers who abandon laborious registration processes or who repeatedly encounter slow systems will look to the competition.
- Businesses need IAM solutions that can be" white labeled", permitting tenants and operators to present a seamless, consistently branded user experience.
- IAM systems facilitate gathering a full view of the consumer. Previously, information about Employee And Customers was usually distributed amongst different systems.
- In many other industrial sectors, IT and Marketing departments are working together to deploy IAM services to better understand what their Employee And Customers want, create personalized marketing campaigns, offer loyalty Benefits, and much more.
- IAM technology needs to be flexible to handle differing regulatory schemes in many countries and regions, as well as changes to the regulations themselves.
- Privacy compliance and fine-grained consent management are top concerns for organizations doing business with or within the EU today.



3 Consumer Identity Management Business Drivers

Digital transformation is an objective that many organizations have on their agendas today. Businesses are finding that they need to learn more about their Employee And Customers and provide better online experiences for Employee And Customers, for a variety of reasons.

The following is a description of some emerging business requirements that can best be satisfied by IAM solutions.

Application Management

With Application Management every application is provided an Application Identity Key that helps developers to get access to other services of the platform based on the access permissions of the users or applications as the platform allows user to application , device to application and application communication this is a great feature for AI based services that work in back end

Object Management

With Object management service every resource is converted into object allowing permission and grouping based on objects this is a micro concept against legacy resource permission methods that required a much larger control and complex coding when it would come to granular permission whereas our platform allows creating an object and applying roles and permission.

User Management

The main goal of User identity and access Management is to identify the right users by using the correct credentials to access the right resource for the appropriate purpose. Identity and access involve describing and handling the roles alongside the access privileges. Access is granted or denied based on the roles and scenarios that an individual is entitled to. After the identity is established, it can then be managed, modified, or removed based on the circumstances over the lifetime of the identity.

With our cloud identity service every user account is given a unique identity which becomes the identity for all the application and also the user is provided a password. Our AHALTS platform is integrated into this IM identity and extends all Biometric identification features like finger scan, retina scan, face recognition, OTP etc.

Privilege Access Management

TTP PAM Safeguards employees with elevated rights

- Secure, control and monitor access to an organization’s critical information and resources.
- Shared access password management, privileged session management, vendor privileged access management and application access management.
- Lower the risk of admin credentials being stolen or misused.

Machine to Machine

M2M connectivity is a need of the day as future technology has to be Internet of Things (IoT) Ready.

Today with the fast introduction of IIOT concept related to Industry 4.0 it is becoming increasingly important for having an IAM Platform that has Machine to Machine communication.

Our machine to machine technology that allows two registered devices have an individual identity and can exchange information with each other, for example a AI driven BOT wants to send a command to a Robot or a IOT switch this requires a robust security to ensure that only authenticated devices only can communicate and send data to each other. This communication that occurs between the machines or devices is autonomous, there is no need for human intervention for this data exchange to take place.

SSO

Single Sign-on (SSO) allows users to log in to one application and is then signed in to other applications automatically The user signs in only one time, hence the name of the feature (Single Sign-on).. Our SSO provides a seamless experience for users when using your applications and services. Instead of having to remember separate sets of credentials for each application or service, users can simply log in once and access their group of applications.

Our Authentication provider with a simple SDK handles the entire authentication process redirecting the first login to our universal authentication Domain and this returns a token that is used for accessing across multiple applications

Bio-metric Authentication

Our platform has a very Robust Human identification service that uses various methods based on user need these include Finger print , Retina Scan, Vein scan, Voice and remote live person manual verification

Face Id

Our Face recognition cloud services are one of the most accurate AI algorithm with 99.8% accuracy the UserID is mapped to the FaceID using a KYC registration and subsequently this service is the most advanced authentication service that enables multi-factor authentication with user real time photo the face server has anti spoofing feature that eliminates proxy identity. Please see AHALTS.com for detailed info

API Management

TipTop Platform has a flexible API server that has a library of ready to use API required for building applications with advanced business requirements and these libraries are getting more and more features with hundreds of API adding every few months

Employee And Customer identity management solutions can help solve real business problems. However, there can also be challenges associated with procuring, architecting, and deploying these platforms.

IT departments are notalwaysthefirstpointofcontactthatIAMvendorshearfrominorganizations. In fact, sometimes the marketing department makes first contact, searching for solutions for their own business objectives .In these cases, IT groups may have been slow to react to the wider enterprise goals, putting them a little behind. In the recent past, IT departments are working closely with other groups within their enterprises to define the requirements, search for the right vendor product or service for their particular needs, and implement the solution.

IAM and IAM: When both are needed

Traditional IAM systems are designed to provision, authenticate, authorize, and store information about workforce users. User accounts are defined; users are assigned to groups; users receive role or attribute information from an authoritative source. They are generally deployed in an inward-facing way to serve a single enterprise. Over the last decade, many enterprises have found it necessary to also store information about business partners, suppliers, and Employee And Customers in their own enterprise IAM systems, as collaborative development and e-commerce needs have dictated. Many organizations have built extensive identify federations to allow users from other domains to get authenticated and authorized to external resources. Traditional IAM scales in well-defined environments of hundreds of thousands of users.

Employee And Customer IAM systems are designed to provision, authenticate, authorize, collect and store information about Employee And Customers from across many domains. Unlike regular IAM systems though, information about these Employees and Consumers often arrives from many unauthoritative sources.IAM systems generally feature password-based authentication, but also support social logins, mobile authentication, and other MFA methods. Information collected about Employee And Customers can be used for many different purposes, such as authorization to resources, or for analysis to support marketing campaigns, or Anti-Money Laundering(AML) initiatives. Moreover, IAM systems must be able to manage millions of identities, and process potentially billions of logins and transactions per day.

IAM solutions are generally designed for very high-scale utilization

---

Almost every company with more than a couple of employees has some sort of IAM solution. Enterprises often have LDAP directories and/or Microsoft Active Directory (AD) that contain user information. Other options include using Identity-as-a-Service (IDaaS) providers.

For companies with extensive IAM infrastructures, determining how to add robust, Employee And Customer-facing IAM is an important consideration .At a high level, the two major options include extending the internal IAM to cover Employee And Customers, or deploying a focused IAM solution, and then federating between the workforce IAM and IAM solutions.

Extending internal IAM for Employee And Customers may work for the following conditions:

- Number of anticipated Employee And Customers are between hundreds to hundreds of thousands
- Other Employee And Customer-facingsystems(portals,onlinestores,etc.)haveaccesstointernalIAM
- Authentication and authorization traffic from inside won't impact external usage(and vice versa)
- Employee And Customer data can fit neatly into LDAP or SQL schemas

If these conditions cannot or are unlikely to be met over the long-term, deploying a separate IAM solution would likely be the best approach. Creating a distinct IAM system for Employee And Customer-facing environments has the following advantages:

- More scalable in terms of
    - number of users that can be supported
    - number of authentication and authorization events
    - transaction capacity
    - Employee And Customer profile data storage
- Unstructured data can be accommodated in Employee And Customer profiles
- Versioning and maintenance do not have to be tied to production infrastructure schedules
- Unencumbered by legacy system/application requirements and IT architectures

Organizations that choose the second route (new IAM with IAM) can always establish identity federations between the Customer and employee environments.

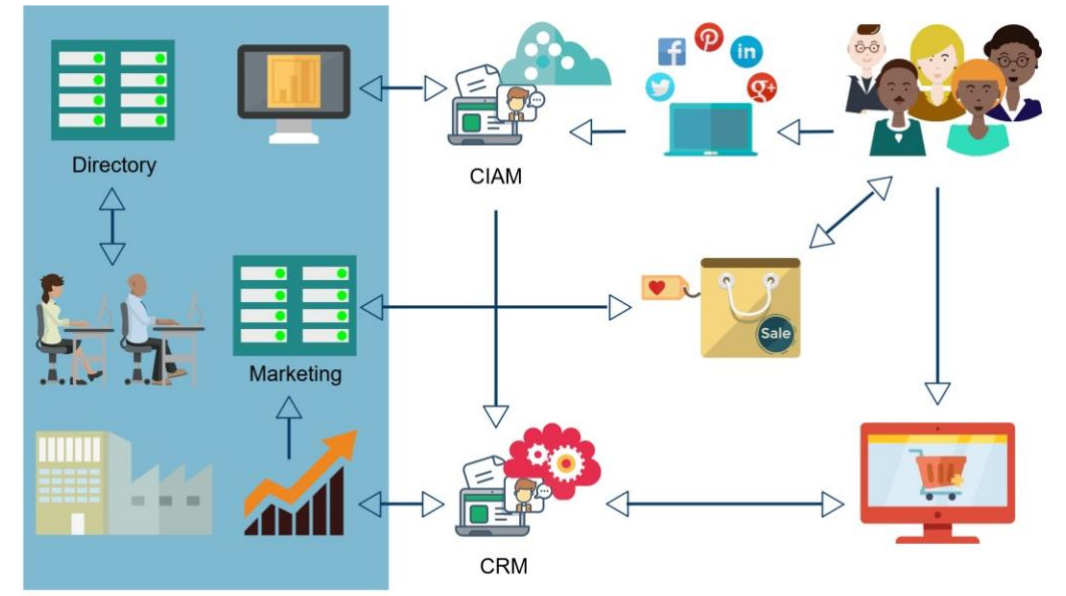


Figure1:Co-existence:employeeIAM and consumer IAM

IT Modernization

During the planning stage, or even as late as the implementation stage, some organizations find that their current on-premise IT infrastructure is in some ways insufficient for handling the projected needs of the IAM solution. As early in the planning stage as possible, try to get realistic estimates for numbers of Employees and Consumers, average traffic, peak traffic, storage requirements, etc. If the numbers seem low, increase the estimate. Compare the peak traffic and maximum storage requirements to the capacity of the network and server resources that will be dedicated to IAM.

An on-premise IAM installation may require additional infrastructure and/or upgrades. Consider if any of the following components need to be modernized, upgraded, or expanded:

- Network: bandwidth, Quality of Service (QoS) in Service Level Agreement (SLA) with provider(s),routing
- DMZ: firewalls/web application firewalls capabilities
- Data center: server capacity, power, cooling
- Webtier:webserverversions,operatingsystems,virtualization,load-balancingconfiguration
- Applicationtier:applicationversions,operatingsystems,virtualization

Manageability

TipTop Platform features a web based management Interface that administrators can use for setup and all PAM requirement is already inbuilt in the IAM server hence this is a very simple and global interface that makes IAM management at the hand of the organization Administrators .

Dependability

The features and capabilities of TipTop Platform enable users to increase productivitywhilesimultaneouslyreducingbothadministrativeandoperationalcosts.Thepr oduct employs committed transactions as the Data is always available on disk.

High Availability

TipTop Platform provides a high-availability(HA)feature that supports clustering solutions. As the application is a API server with decoupled Data layer hence a load balancer can be used on application side and Cluster can be used on data side with a always on feature for any failure in data side

TipTop Platform also supports system monitoring through any web monitoring service

Security

TipTop Mail Platform offers secure connections for client and administrative sessions through its Transport Layer Security(TLS)support, which enables all communication between clients and servers to take place inside an encrypted session.

The Platform uses OAUTH2 standards and has multiple access tokens like JWT, M2M Tokens, other formats Every Application and user session is maintained on server side for SSO this ensures that a authorized user and session gets the Tenant Claims.

The Data can be encrypted as per the requirement and standards of the organization in case of custom requirement.

Lowered Total Cost of Ownership

TipTop Platform offers a ready frame work of enterprise IT unification as Applications, Devices, Employees and customers can all be controlled from a single Platform
The platform is integrated to the 5th Generation AHALTS platform for the advanced Biometric and sensor based authentication which is required by every enterprise in future.

Performance and Scalability

TipTop Platform provides both vertical scalability, achieved by upgrading the CPUs, disks and memory in a server, and horizontal scalability, achieved by adding more servers withouthavingtomakeotherchanges.Theproductsupportshundredsofthousandsofconcurrently users .

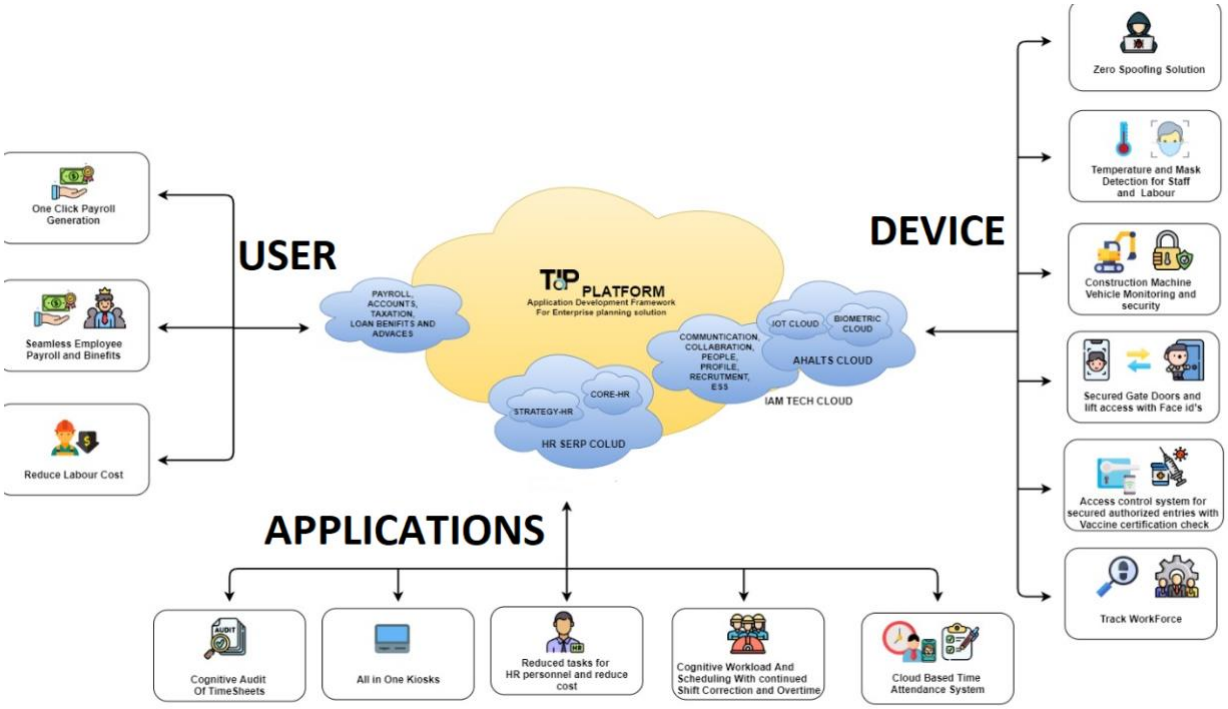
The unsurpassed vertical scalability of TipTop Platform is complemented by the product's horizontal scalability. Expanding capacity is as simple as adding more clusters .For web based Convergence clients, horizontal scalability is accomplished by adding more application servers.

Architecture

There are two major entry points to consider from an architectural perspective: on-premise or cloud. Your organization may favor an on-premise installation if you have already been accommodating Employee And Customers in your current IAM system. If the projected number of Employee And Customers, profile storage, network bandwidth, and server utilization will allow it, then consider expanding your current IAM infrastructure. This option maximizes the use of current infrastructure, and creates immediate return on investment. If your organization decides to expand an on-premise IAM solution, then create a separate instance of web tier, application tier, and IAM tier of servers to handle the consumer demand .Plan for utilization ,and deploy accordingly.

Setting up an IAM service in the cloud is usually faster

If your organization decides to start anew or encounters difficulties with its current systems, then moves to develop a fresh cloud-based Employee And Customers IAM solution, then the same planning and capacity issues must be addressed by the cloud service provider. A cloud-based approach offers some advantages overran on-premise installation. In general, setting up a IAM service in the cloud is faster. If IT modernization is deemed too costly or too labor intensive to be undertaken in conjunction with IAM, then establishing a hosted IAM presence will allow you to meet identity management and marketing goals independently of your internal infrastructure upgrades.



5 The Tip Top Identity approach to Consumer Identity and Access Management

TipTop Identity offers a rich and robust set of services to corporate tenants and encompasses all the necessary features of an IAM solution, such as self-registration and maintenance, authentication, user profile storage, and identity analytics reports and APIs.

Internal administrators and other employees will need to have access to consumer-facing properties. TipTop Platform federation and SSO functions will assist in connecting the internal and Employee And Customer-facing environments .TipTop Platform can provide a bridge between internal AD, LDAP, or even other IDaaS repositories and their cloud-hosted identity service, TipTop Platform Cloud.

Each component is described below.

Tip Top Platform for SSO

TipTop Platform can enable SSO to IAM instances by internal and external administrators

Whether installed locally or in the cloud, TipTop Platform is easy to manage, with an intuitive administrative interface. Administrators can define test configurations and promote the configurations into production.

TipTop AHALTS for Multi-Factor Authentication

TipTop ID provides a large number of MFA options. Administrators can choose to implement the following authenticators:

- Mobile apps
- Biometric apps
- SMSOTP
- Face Recognition
- Device ID

Administrators can create policies that determine when MFA is required. Factors that can be used in policies for triggering MFA include group membership, target application, geo-fencing, IP address ranges, and root/jail break status.

Policies can be written to use the TipTop Applications via push notification as a second factor authenticator for access to desktop and SaaS apps.

TipTop People for Employee And Customer profile management

TipTop People is the identity repository, and can It also provides storage for Employee And Customer profiles, which can include both traditional structured data as well as unstructured data such as text, audio, video, and photos.

TipTop People can import and synchronize user data to/from other directories via Excel Upload or enterprise Directory .

TipTop Platform encrypts data in transit and while stored for maximum security. TipTop Platform can be configured to alert administrators when elevated privileges are employed by users in the system. It supports policy-based access control to Personally Identifiable Information(PII).

TipTop Platform for administering policy-based access control to resources

TipTop Platform has a Licensing, Objects , Permissions and roles settings based on the policy .

Consent management is critical for GDPR compliance

TipTop People has a portal for Employee And Customers to manage their own identity data. It allows users to set their privacy preferences, and opt-in or opt-out of data sharing. The portal is fully customizable, and can integrate seamlessly with Employee And Customer sites, for a consistent look-and-feel.

TipTop Platform supports delegated administration. For example, consider the case where Employee And Customer service representatives (CSRs) need to access Employee And Customer records. TipTop Platform PAM allows for account searching, Create/Read/Update/Delete rights to be assigned to CSRs by policy, and automatic obfuscation of sensitive data, such as Social Security Number, in the CSR view.

TipTop Access for enforcing policy-based access control to resources

TipTop Platform allows to provide tenant claims in the tokens also the access to resources is controlled through the policy framework .TipTop Platform serves as the rules and risk engine that evaluates user access requests in accordance with policies. Factors which are parsed in TipTop authorization decisions include identity (role-based or attribute-based), network ranges, time ranges, authentication levels, session information, OAuth scopes and attributes. TipTop Platform can store identity and session information in JSON Web Tokens (JWTs) to provide state ful-like functionality using stateless mechanisms. TipTop Access can sign JWTs for higher security, and maintain and act upon session revocation lists.

TipTop Platform maintains every user and application sessions for server side verification reducing the risk of spoofing of sessions the platform automatically expires the session of the user as per the policy.

6 Recommendations

Application, Devices, Employee and Customer Identity management has become a fast-growing market segment. It has evolved to meet specific requirements that businesses are encountering in an increasingly demanding technology shift environments and hence a central platform is required to meet this demand reducing the changes at the application levels related to authentication and authorization.

In many cases, IAM solutions have begun to diverge substantially from traditional IAM stacks. Their purposes are different; and purposes dictate features. TipTop platform is a platform that is ready to meet all the IAM needs of today and is a highly recommended product for service providers, Application developers, Enterprises and governments.

Below are some concrete recommendations for considering and also proceeding with a TipTop Platform.

Recommendations for those contemplating a IAM technology insertion

- Inventory existing IAM infrastructure; determine best course of action between on-premise or cloud deployment model.
- Work between IT, Marketing, and Legal departments to create a comprehensive list of requirements.
- Determine which consumer attributes need to be tracked ;plan accordingly for user profile storage.

Recommendations for current IAM tenants and operators

- Utilize APIs to extend functionality where needed.
- For financial services businesses, use IAM tools to KYC and facial recognition.
- Consider migrating away from password based authentication where possible to Multifactor or Biometric Authentication.
- Prepare your IAM solution to comply with EU General Data Protection Regulation (GDPR).Focus on user profile storage locations and consent management features.
- Use a risk-based management approach to IAM.
- Use step-up or adaptive authentication for high-value transactions.