Universal Identity Services

Service Description

Version 1.4
December 13, 2012
# Table of Contents

**Introduction** .......................................................................................................................... 1

- Universal Identity Services Overview ....................................................................................... 1
- Key Components of Universal Identity Services ................................................................. 1
  - Identity Proofing .................................................................................................................. 1
  - Authentication ..................................................................................................................... 2
- Digital Signature Services ........................................................................................................ 2
- UIS Mobile Application and ID Message Center ............................................................ 3
- Enterprise Dashboard ............................................................................................................. 3

**Technology Overview** ........................................................................................................... 4

- Elements of the Service ........................................................................................................ 4
- Network Architecture .......................................................................................................... 5
- Geographical Locations ........................................................................................................ 6

**Service Package** .................................................................................................................... 6

- User Credentialing ................................................................................................................. 6
- Loading User Data ................................................................................................................ 8
- Registration and Identity Proofing .......................................................................................... 9
- Token Issuance ..................................................................................................................... 10
- Digital Signature API .......................................................................................................... 10
- Credential Renewal/Maintenance ......................................................................................... 11
- Revocation/Cancellation of a Token ...................................................................................... 11
- Authentication ...................................................................................................................... 12
- SAML-based Authentication ................................................................................................. 12
- Authentication for Web Applications .................................................................................... 12
  - UIS Performs all Authentication Processes ..................................................................... 13
  - UIS Authenticates Users Using Customer-held Data ......................................................... 14
  - UIS Provides Second Factor Authentication Only .......................................................... 15
- Administrator Tasks ............................................................................................................. 15
- Bulk Upload of Users ............................................................................................................ 15
- UIS Dashboard for Administrators ...................................................................................... 16
  - User Report ....................................................................................................................... 20
  - Registration Report .......................................................................................................... 20
  - User Detail Report ............................................................................................................. 20
  - ID Proofing Report ............................................................................................................ 22
  - OTP Device Registration Report ...................................................................................... 23
  - OTP Device Activity Report .............................................................................................. 24
  - Hardware Token Report .................................................................................................... 24
- APIs Supported ...................................................................................................................... 24
- Standards ............................................................................................................................... 26
  - OATH .................................................................................................................................. 26
  - SAML ................................................................................................................................. 26
  - SPML .................................................................................................................................. 26
  - LDAP .................................................................................................................................. 27
  - PKI ...................................................................................................................................... 27
  - Branding ............................................................................................................................. 27

**Service Management** ............................................................................................................. 27

- On-boarding ........................................................................................................................... 27
- Discovery and Analysis .......................................................................................................... 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>27</td>
</tr>
<tr>
<td>Deployment Campaign</td>
<td>27</td>
</tr>
<tr>
<td>Professional Services</td>
<td>28</td>
</tr>
<tr>
<td>Service Commencement</td>
<td>28</td>
</tr>
<tr>
<td>Service Termination</td>
<td>28</td>
</tr>
<tr>
<td>Service Levels</td>
<td>28</td>
</tr>
<tr>
<td>Change Control</td>
<td>28</td>
</tr>
<tr>
<td>Service Monitoring</td>
<td>28</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>29</td>
</tr>
<tr>
<td>End-user Support - Tier 1</td>
<td>29</td>
</tr>
<tr>
<td>Tier 2 Support</td>
<td>29</td>
</tr>
<tr>
<td>Verizon Responsibilities</td>
<td>30</td>
</tr>
<tr>
<td>Security Services Advisor</td>
<td>31</td>
</tr>
<tr>
<td>Customer Responsibilities</td>
<td>31</td>
</tr>
<tr>
<td><strong>Security Controls</strong></td>
<td>32</td>
</tr>
<tr>
<td>Separation of Data</td>
<td>32</td>
</tr>
<tr>
<td>Data Protection</td>
<td>32</td>
</tr>
<tr>
<td>Network</td>
<td>33</td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery</td>
<td>33</td>
</tr>
<tr>
<td><strong>Terms and Definitions</strong></td>
<td>33</td>
</tr>
</tbody>
</table>
Introduction

Universal Identity Services Overview

Organizations today face the complex challenge of controlling costs and reducing complexity and risk, while simultaneously providing a positive identity authentication experience for users. Verizon Universal Identity Services (UIS) is designed to create an easy-to-use online experience to help organizations securely and cost effectively addresses these challenges, without having to implement expensive, complex technologies.

UIS is a cloud-based identity-as-a-service solution that includes identity proofing, credential issuance, strong authentication, and digital signature services. UIS shifts complexity from the organization’s IT Department to Verizon—allowing the organization to still retain control of access management. Services that now take organizations weeks to perform can be handled in minutes — without paper-based processes or manual updates for multiple applications.

UIS provides,

- On-demand identity-as-a-service, without the complexity and expense of on-premises hardware and software
- Strong authentication solution from Verizon, the first Identity provider to earn Identity, Credential and Access Management (ICAM) Level 3 certification.
- Cloud-based identity solution that helps reduce the risk of identity fraud by providing real-time transactional identity assurance
- NIST Level 3 compliant ID Proofing and Authentication services
- Rapid-deployment, fast identity proofing and credential issuance
- Positive user experience for credential provisioning and transactional authentication
- Standard authentication experience across all applications

Key Components of Universal Identity Services

Identity Proofing

UIS includes identity proofing in a fully electronic process. We support online antecedent processes, enterprise antecedent data load or a bulk upload using web services. After users complete identity proofing, they can update their information, reset passwords and PINs in a fully electronic process, and register new authentication credentials such as a new email or new mobile device. For administrators, UIS includes an interface to enable customization and a dashboard for tracking service use. Key features include:

- Simple integration into existing systems to leverage identity data and account directories
- Customizable enrollment screens and workflows
- Administrative interface for registration workflows and form factor configuration
- Administrative dashboard for tracking service use
- Support for automated online knowledge-based assessments and in-person identity vetting
- Support for self-service Notary via secure e-fax and in-person Trusted Agent identity vetting
- Meets requirements for NIST Level 3 identity proofing
Credential Provisioning UIS enables users to use credentials they already have—such as an email or a mobile device. Organizations can choose specific credentials or can simply enable all UIS options. We support phone calls, text messaging, and interactive voice response (IVR) around the globe. Key features for credential provisioning services include:

- Low-cost, flexible online process for credential provisioning up to NIST Level 3
- Multiple assurance-level authentication
- Support for many authentication approaches, including: username/password, one-time passwords sent to a mobile device using text messages or interactive voice response (IVR), one-time passwords (OTP) sent to landline phones using IVR, OATH hardware and software tokens, PINs or passwords with the mobile application, and more
- Enables user preferences for OTP delivery
- International phone support includes phone calls, SMS, and IVR from over 200 countries

Authentication

UIS provides a strong, yet flexible, authentication gateway. UIS supports enterprise and user preferences for delivery of one-time passcodes within timeout and lockout policies—limiting organizational risks. UIS includes support of SAML 1.x—2.0, and Juniper Networks or Citrix VPN support via SAML. With the mobile application and the ID Message Center, users can access and approve transactions anytime, virtually anywhere. Users have an easily accessible record of past transactions—approved and rejected—as well as pending transactions. Enterprises can enable an online version of the ID Message Center, providing the same features as the mobile application. Key features include:

- Managed authentication
- IP malice and IP geo-location integrated with authentication
- Mobile application with ID Message Center enables access anytime, virtually anywhere
- Web services toolkit for online ID Message Center enables online tracking of pending, accepted, rejected, and expired authentication transactions
- Compliant with requirements for NIST Level 3 authentication
- Help Desk support for Tiers 1-3, 7x24, or customizable support (e.g. Tier 3 only)
- Organizations shift complexity for strong authentication to Verizon while retaining control of access management

Digital Signature Services

Universal Identity Services includes digital signature services that enable organizations to apply digital signatures to essential corporate documents and Adobe PDF files, such as employment, financial, or other materials. The digital signature on a document is legally recognizable as a wet signature. Key features include:

- EU qualified certificates that can be used for authentication and digital signing
- Digital signature interface for end users
- Digital signature solution that helps healthcare companies meet the DEA Electronic Prescriptions for Controlled Substances Rule (EPCS)
- Enterprise toolkit for digital signing services to integrate with web applications
- Digital signature API enables signing of PDF documents or the document hash
UIS Mobile Application and ID Message Center

UIS includes a mobile application that is available on BlackBerry (touch and non-touch), Google Android, Microsoft® Windows® Phone, and Apple iOS devices (iPhone, iPad, and iPod Touch). This mobile application provides an OATH soft-token for providing one time passwords to authenticate a transaction. Users access the mobile application by providing their PIN, which they define as part of registering their UIS identity. UIS combines the user-supplied PIN with the OTP, and authenticates the user to their ID Message Center queue of transactions.

The ID Message Center is a value-added feature of the mobile application. Here’s how it works:

- Each transaction from the relying party is sent to the ID Message Center.
- Similar to an inbox in an email application, the user performs a task for each transaction. Transactions are organized into Pending, Approved, Rejected, and Expired tabs.
- The relying party defines the level of assurance and authentication credentials required for a given transaction. For example, the relying party can simply allow the user to accept the transaction, and UIS sends the unique device ID, the unique OTP, and the user-entered PIN to authenticate the transaction.
- The relying party can also request a real-time password, or a real-time entry of the PIN, and then UIS sends these credentials along with the transaction. The relying party also defines the expiration time for a given transaction.
- Finally, the relying party can submit the transaction to the user’s ID Message Center queue, where it waits for the user to access it. Or, the relying party can send a push notification to the user, which sends an immediate pop-up notification to the user’s device. Push notifications are valuable in time-sensitive activities, such as enabling login to a corporate application with a timeout feature.

Enterprise Dashboard

Enterprise clients with appropriate privileges can utilize the reporting dashboard to view information that is specific to their own environment, users and user’s activities. Administrators can access all information in the Summary, Service, Reports and Alerts tabs in the dashboard.
Technology Overview

Elements of the Service

The UIS platform consists of UIS Core Services, UIS Signature Services and the UIS Credential Management Backends.

UIS Core Services

- Registration Service, which supports three registration mechanisms: user self-registration, registration via web services and registration via bulk file upload. The service can be configured to access customers’ directory services and the services of third party identity proofing providers. Depending on the type of credential, the Registration Service also handles provisioning and management of credentials.

UIS Signature Services

- Signing Service

UIS Credential Management Backends

- OATH, SMS etc
- Third Party Identity Proofing Providers
- Customer’s Directory
- SMS Provider
- IVR (Voice)

Figure 1: Overview of UIS

UIS Core Services consist of two main parts:
UIS Digital Signature Services provides a web services API to support client software enabling users to sign PDF documents and XML transactions. Users’ keys and certificates are held centrally by UIS.

UIS Credential Management Backends provide support for the different types of credentials. The Backends may need to access third party providers, for example to send SMS messages containing one time passwords. In addition to supporting more typical authentication credentials, such as SMS or IVR OTPs, Verizon’s UIS also includes a mobile application that provides a OTP. This mobile app displays an ID Message Center, where users can review and approve authentication transactions.

Network Architecture

UIS is a cloud-based service that is accessed via the Internet and does not reside on the customer's MPLS/PIP network. Based on a high-availability architecture, UIS runs in multiple data centers so in the event of a disaster, services are quickly switched to another data center without affecting DNS names or relevant URLs. Additionally, UIS employs multiple layers of security defense to deter threats and data breaches.
Protocols used are as follows:

HTTPS is used for connections between UIS and User Administrators, Automated Administrators, Users and Authentication Requestors.

LDAP or LDAPS is used for connecting UIS to Customer’s directory services. A VPN may be used to help protect connections to a customer’s Microsoft Active Directory® service.

Geographical Locations

UIS is delivered via the cloud and the high availability, reliable infrastructure currently operates in Verizon’s Culpepper, Virginia and Miami, Florida. Data centers. UIS customers can be located in one country and have users in many different countries. Customers should consider legal, data protection and export compliance issues. UIS is currently available to customers in the U.S. and Europe. See your Verizon account manager for details.

Service Package

User Credentialing

The UIS registration process is configurable and consists of the following steps:

**Invitation:** The customer uploads a list of users to UIS and emails are then sent to those users inviting them to register.

**Registration:** There are three primary ways that users can register.

1. CSV file upload – A CSV file containing information on all users to be credentialed is uploaded to UIS. The list is then approved by the UIS administrator and a registration invitation email is sent to the users.

2. Registration via Web Services – customers can initiate the registration process through web services.

3. Click-through registration – UIS implementations that utilize SAML toolkits allow users to register via a direct click through registration process.
Identity Proofing:
Using UIS, organizations can identity proof their users using one of six different methods described below:

- **Enterprise**: Verizon will confirm the validity of the user’s identity by verifying the username provided by the user and a password against an enterprise directory. This method of identity proofing results in a NIST Assurance Level 1 – Remote unless separately certified by the customer.

- **NIST Assurance Level 2**: Verizon will confirm the validity of the user’s identity by verifying information provided by the user against public and private external data sources. This process will meet the requirements of NIST Special Publication 800-63-1 for Identity Proofing Requirements for Assurance Level 2 - Remote.

- **NIST Assurance Level 3**: Verizon will confirm the validity of the user’s identity by verifying information provided by the user against public and private external data sources. This process will meet the requirements of NIST Special Publication 800-63-1 for Identity Proofing Requirements for Assurance Level 3 – Remote.

- **Trusted Registration Agent**: Verizon will confirm the validity of the user’s identity by directing them to a Trusted Registration Agent. Such Agents go through an identity assurance procedure that will inspect a user’s physical identity documents. This method of identity proofing results in a NIST Special Publication 800-63-1 for Identity Proofing Requirements for Assurance Level 3 – In Person.

- **Notary Public**: Verizon will confirm the validity of the user’s identity by directing them to a Notary Public. Such Notary Publics verify the user’s identity by inspecting a User’s physical identity documents and notarizing the Verizon supplied Identity Proofing Form. This method of identity proofing results in a NIST Special Publication 800-63-1 for Identity Proofing Requirements for Assurance Level 3 – In Person.

- **Enterprise Antecedent**: This method of ID proofing allows companies to ID proof employees using their own approved methods, and submit these ‘pre-vetted’ users to UIS so they can be added into UIS by the Trust Registration Agent (RA) with the appropriate vetting level. This takes advantage of the fact that the company for which these users work has already vetted their employees through an approved (country specific) process and/or i9 process in the US. The use of this capability allows those vetted employees to be assigned a UIS ID at the appropriate assurance level (by the UIS RA) without an additional manual vetting process as part of UIS registration.

Credential Issuance:
Users may be issued a second-factor authentication device. The precise details of the registration flow are provided to the customer during the implementation process.
Loading User Data

Information on users can be loaded in bulk using the following process:

![Diagram of Bulk Loading of CSV Files](image)

Figure 3: Bulk Loading of CSV Files

Alternatively a web services interface can be used:

![Diagram of Bulk Loading using API](image)

Figure 4: Bulk Loading using API
Registration and Identity Proofing

The diagram below explains the UIS registration and identity proofing processes.

Upon receiving an email registration request, users can confirm their identity and provide a UIS system password. They select which one-time password (OTP) devices they want to use and may be required to supply details about the devices (e.g. mobile phone number).

As an optional step, users can be further verified using antecedent data. Antecedent data may be derived from the initial bulk load of user data or a variety of trusted external sources, in strict accordance with the requirements of NIST 800-63. For LOA3, the user is required to correctly answer a number of knowledgebase questions within a specified period of time.

In the event that knowledge-based questions are insufficient to verify a user’s identity, the physical inspection of identity-related documents can also be utilized. A Trusted Registration Agent (RA) may be used to confirm a user’s identity and this typically involves the physical inspection of documents such as an I-9 or a driver’s license. If satisfied, the Agent, who also must have proper UIS credentials, uses the UIS portal to approve the user’s registration request. If the verification of an identity is to be performed by a public notary, UIS provides the user with instructions on how to proceed by visiting a notary and providing a Trusted Registration Agent with notarized documentation. The Agent then uploads this documentation to UIS as a .pdf file.
Token Issuance

Once the user’s identity has been verified, the next step is for the user to create and obtain an identity token that can be used to access customer applications. UIS supports several authentication methods, the most common option being the use of a one-time password (OTP). Verizon provides users with a choice of OTP authentication form factors to suit their own personal preferences, although customer organizations may restrict their users to specific methods. Options include:

- **SMS-OTP**: No issuance is necessary as UIS only requires the mobile phone number of the user. UIS checks that the mobile number is correct by sending an OTP to the number and the user responds to UIS with the OTP. UIS supports telephone numbers for over 190 countries. The service includes the cost of sending the SMS messages, although users may be charged by their carrier for receiving these SMS messages.

- **Email-OTP**: No issuance is necessary as UIS only requires the email address of the user, which has already been provided. An OTP is sent to the user's email address and the user then responds to UIS with the OTP.

- **Interactive Voice Response (IVR-OTP)**: No issuance is necessary as UIS only requires the phone number of the user. International calls are also fully supported, although users pay for the calls. UIS calls the user on the supplied phone number and provides an OTP, the user then responds to UIS with the OTP.

- **Mobile Application**: Users are given instructions on how to download, install and initialize the OATH-based, mobile application. The application is supplied and supported by Verizon as part of the UIS service.

- **Soft Token OTP**: The soft token is a version of the mobile application that has been designed to run on a “PC” (desktop or laptop) to be used as an OTP generator. This application is provided by and supported by Verizon as a part of UIS. This application is OATH-based.

- **VASCO DIGIPASS Hardware Tokens**: These are OATH-based. For software-based tokens the user is given instructions on how to download, install and initialize the application. The application is provided by and supported by VASCO. For hardware tokens, Verizon will ship the token to the end-user as long as this is permitted by export compliance regulations. Verizon retains ownership of tokens but the customer assumes responsibility for user compliance with laws and regulations.

If the user is to be able to digitally sign documents, they will also be issued a credential with a signing key and certificate which is held by UIS.

**Digital Signature API**

UIS supports the generation of keys and X.509 certificates as part of the user credential issuance process. Certificates are only issued from UIS-compatible certificate authorities. UIS holds the users keys and certificates within UIS so signatures cannot be made when the keys and certificates are in other key stores.

Users can also access the UIS ID Message Center available in the mobile application. The mobile application is available for Android, BlackBerry (touchscreen and non-touchscreen), and iOS (iPhone, iPad) devices. For end-users, the ID Message Center displays pending, accepted, and rejected
transaction requests. With this feature, end users can track their activity. For enterprises, UIS provides a toolkit to enable the ID Message Center for employees.

Credential Renewal/Maintenance

User and Token Administrators, selected by the customer, can access the Administrative Console to manage UIS credentials that require renewal (hard tokens). Users can also maintain their credentials via the UIS portal and manage their profile in a number of ways:

- Modify mobile numbers
- Modify email addresses
- Request a new credential
- Turn off one token type (e.g., SMS-OTP) and turn up another token type (e.g., Email-OTP)

The UIS service does support the use of OATH based hardware tokens. These are issued to users in cases where an organization has selected them as a form factor to provide to their employees. If an issue arises with the hardware token an end user will be required to go through their support desk for a replacement or to have it reset.

Thus if a user:

- replaces a mobile phone which has a soft token or mobile application
- loses a hard token or finds that their hard token has failed
- requires a credential with a new form factor,

then the user may request a new token of the appropriate type.

Revocation/Cancellation of a Token

At any time users may go to the UIS portal and remove one of their credentials:

- turn off one credential type (e.g., SMS-OTP) and turn up another credential type (e.g., Email-OTP)

This is normally used when a user:

- loses a mobile phone which has a soft token or mobile application
- loses a hard token or finds that their hard token has failed

Authorized Administrators may also use the UIS portal to remove a user’s credential.
Authentication

The UIS Identity Broker is a real-time identity authentication and identity risk assessment service. The Identity Broker allows a customer application (usually a login screen to a VPN or application) to send a query requesting that the user’s identity be authenticated. This authentication includes an assessment of the status and authenticity of the user’s identity credentials along with other transactional information of the user currently attempting to login to that customer service or resource.

Typical transactions that use the UIS Identity Broker to authenticate users include VPN access, network logon, Web logon, service and direct authentication against online Software-as-a-Service (SaaS) applications.

Users must enter their userID and password before the UIS Identity Broker can determine which second factor authentication mechanism is to be used. The preferred authentication method is selected by the user at registration. Additionally, customers can choose to limit the authentication methods available to an end user. If the user’s preferred method is not available, a pre-registered back-up method may be selected by the user at the time of authentication. If the user’s credentials do not pass the authentication tests, the transaction is reported back to the customer application as having failed to authenticate.

UIS can be configured to perform further tests on a per-relying party basis:

- **Location and Behavior Tests** – The Identity Broker service will also assess
  a) if the IP address is on the IP Watch List, and
  b) if the geographic location of the IP address is a banned country

SAML-based Authentication

Products, services and applications that support either SAML 1.x or SAML 2.0 can use UIS to authenticate users. UIS supports decomposable SAML assertions as well as configurable assertion attributes per relying party. UIS also offers Java, .Net and Ruby toolkits for SAML.

Authentication for Web Applications

Customers can help protect their web applications using pre-configured UIS toolkits, which are supported and maintained by Verizon. There are three methods of authentication for web applications.
UIS Performs all Authentication Processes

Authentication is performed entirely by UIS using UIS-held data.

Figure 6: UIS provides all authentication processes
UIS Authenticates Users Using Customer-held Data

UIS checks userid and password stored in the customer's directory service and then performs second factor authentication.

Figure 7: UIS Authenticates Users Using Customer-held Data
UIS Provides Second Factor Authentication Only

In this method, the customer’s web application checks the userid and password and only uses UIS to perform second factor authentication.

![Diagram of UIS Providing Second Factor Authentication Only](image)

**Figure 8: UIS Provides Second Factor Authentication Only**

Administrator Tasks

The administrative roles for UIS are managed and maintained by the Verizon Service Management organization.

**Bulk Upload of Users**

UIS administrators can upload CSV bulk files that contain user information.
UIS Dashboard for Administrators

UIS administrators can use the web-based dashboard to view summary, service, alert and other reporting information.

Administrators can also view logs, reports and statistics from the perspective of all customers, a specific customer and/or a group of specifically selected customers. This enables administrators to quickly and easily view, review and understand the activities as they relate to each specific relying party.

Relying Party Administrators must be created and granted appropriate permissions to view dashboard reports for their own Relying Party and users, by the Verizon UIS Engineering organization.

The following sections highlight the information available on the dashboard.

Figure 9: UIS Dashboard
Administrators can drill down into the information by:

- Authentication mechanism
- Geographic region
- Assurance levels
- Service type
The Services screen shows:

![Welcome to Universal ID Manager](image)

**Figure 11: UIS Dashboard Services**
Administrators can drill down to find details of services of statistics.

![Figure 12: UIS Dashboard Reports Screen](image)

Administrators can select filters to create reports. Reports can be produced and downloaded (in Microsoft Excel® or pdf formats).

The Alerts screen shows:

![Figure 13: UIS Dashboard Alerts Screen](image)
Administrators can search for alerts using:

- Alert type
- Authorization Method
- State
- Service
- Date range
- Status

Alerts can be edited and deleted.

**User Report**

A User Report is available in the Summary Section of the dashboard and includes a tabular view of the following user-related information:

- User name
- Number of request
- Number successful
- Number failed
- Time and date of last successful login

The information in the table can be saved and exported as a .pdf, .csv or .xlsx file.

**Registration Report**

The Registration Summary Report enables administrators to quickly see summary statistics on end-users registrations at each customer site. This report is displayed in a chart format and is included in the Summary Tab on the dashboard.

Report information indicates:

- Number of users sent ‘registration invitation’ and/or uploaded via CSV
- Number of users that have completed the registration process
- Number of users that have been authenticated after having successfully registered.

**User Detail Report**

This report is available in the “Summary” section of the dashboard as a table displaying:

- Relying Part CD
- Person ID
- IA APP ID
- First Name
- Last Name
- User Name
- Email
- Description (active / inactive)
- Registration Status
- Registration Workflow (NH, ZFR, etc.)
- Activation CD (ex: H29P8650)
• Activation Date
• RP assurance level
• Assurance Level ID (user level)
• Create Date
• Cert Request Date (as applicable)
• Cert user name (as applicable)
• Approval status (of cert, as applicable)
• Cert ID (as applicable)
• Subscriber Agreement Date (as applicable)
• RA approval Date (as applicable)
• Cert Serial Number (as applicable)

Figure 14: UIS User Detail Report
ID Proofing Report
This report is available in the “Summary” section of the dashboard as a table displaying:

- UUID
- Application ID
- Registration Status
- Attained Assurance Level
- User name
- KBA Test status (Pass or Fail)
- Relying Party name
- Relying Party code
- Relying Party type
- Requested Assurance Level
- Date
- Source (choice point, etc.)
- Background Validation
- Registration Workflow

Figure 15: UIS ID Proofing Report
OTP Device Registration Report
This report is available in the “Summary” section of the dashboard as a table displaying:

- IA APP ID
- User name
- REG_STATUS
- OTP_TYP_NM
- Name
- VERIFIED_DEVICE
- OTP_VAL
- OTP_UUID

Figure 16: UIS OTP Device Registration Report
**OTP Device Activity Report**
This report is available in the “Summary” section of the dashboard as a table displaying:

- OTP Device type
- Attempts Successful
- Attempts Failed

![UIS OTP Device Activity Report](image)

**Figure 17: UIS OTP Device Activity Report**

**Hardware Token Report**
This report is available in the “Summary” section of the dashboard as a table displaying:

- User ID
- First Name
- Last Name
- Email
- User Enabled
- User Locked
- User Last Authentication Date
- Token Serial Number
- Token Enabled

**APIs Supported**
The following set of APIs are available for use by Verizon Professional Services to assist in the customization of the standard UIS registration, ID proofing, authentication and profile management user interfaces.
Also, the APIs can be used to create custom integrations and/or integrate custom / 3rd party ‘front end’ applications to meet specific customer needs, using UIS on the back-end for ID proofing, credential issuance, authentication and/or digital signing capabilities.

<table>
<thead>
<tr>
<th>Name of API</th>
<th>End User Functionality That Can Be Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS API (Public)</td>
<td>Allows digital signing capabilities to be added to a 3rd party application</td>
</tr>
<tr>
<td></td>
<td>Using the DSS API the following types of signing are supported:</td>
</tr>
<tr>
<td></td>
<td>• Signing of a PDF document</td>
</tr>
<tr>
<td></td>
<td>o The PDF is sent to the signing service, which then sends a hash of the PDF to VM Ware TriCipher Armored Credential System (TACS). The Digital Signing Service does prep and authentication prior to the signing, and performs any post-processing that is required. All signing operations happen within the TACS crypto module, as this is where the user's private key is securely stored.</td>
</tr>
<tr>
<td></td>
<td>• XML signing</td>
</tr>
<tr>
<td></td>
<td>o IDMC uses DSS with XML signing / prescription flow signs an XML document.</td>
</tr>
<tr>
<td></td>
<td>• Hash Signing</td>
</tr>
<tr>
<td></td>
<td>o Using the Adobe Plug-in. The Adobe Plug-in signs a hash of the PDF, leveraging functionality of the Authentication Gateway and Digital Signing Service</td>
</tr>
<tr>
<td>IDMC Web API (Private)</td>
<td>• Allow customers to implement a ‘delivery’ and ‘signing’ capability into their application.</td>
</tr>
<tr>
<td></td>
<td>• Generically to send a ’text’ to a user, and have the user approve or reject it; after which it sends the response back to the originating application.</td>
</tr>
<tr>
<td>Registration Status API (Private)</td>
<td>• Provide status of user registrations</td>
</tr>
<tr>
<td></td>
<td>• A custom call that a Relying Party (RP) can make regarding a user (enterprise ID) to determine the status of their registration</td>
</tr>
<tr>
<td></td>
<td>• For example: An RP has uploaded users, and they want to know which users are in which process. They make a ‘call’ and ask for enterprise ID / username and it returns the status.</td>
</tr>
<tr>
<td>Credential Management API (Private)</td>
<td>• Allows customers to write and/or create their own personalized, customized UI for registration and/or profile management</td>
</tr>
<tr>
<td></td>
<td>• Would be completely independent from the UIS registration and Profile Manager, and only use the back-end UIS</td>
</tr>
<tr>
<td></td>
<td>• Allows customers to write their own Profile Management and registration screens</td>
</tr>
<tr>
<td>Name of API</td>
<td>End User Functionality That Can Be Created</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ID Proofing API (Private)                            | • Used if a customer wants to write their own R registration UI (and not Profile Management UI)  
• Used to vet someone at any level. It can be used in isolation for just ID proofing / registration. This differs from the Credential Management API in that is only for registration, and does not relate to Profile Management.                                                                                   |
| Authentication Gateway API - updated (Private)       | • Allows customers to write / customize their own authentication screens, and not use the UIS authentication screens.  
• Often used if customers want their own custom terminology in the authentication screens.  
• If a customer wrote their own user login screens, then they need to use this API to authenticate the users based on the single, multi and second factors.                                                                                                                                                                      |
| Device API (Private)                                 | • This API can provide an authentication screen 'remember my device' check, through a server side cookie.  
• This remembers the device the user logged in from, so the next time they need only to enter the password and don't have to enter the username.                                                                                                                                                                |

**Standards**

**OATH**

UIS provides credential provisioning and authentication services for OATH hardware tokens and OATH software tokens. With this support, UIS enables strong two-factor authentication with a wide range of devices. The mobile application is available on iOS (iPhone, iPad, iPod Touch), Android, and BlackBerry mobile devices. By supporting devices that users are likely to already own, UIS helps manage the cost and reduce complexity of having dedicated tokens, USB fobs, or other additional authentication devices.

OATH v1.0 is defined by rfc 5849.

**SAML**

Both the W3C standards SAML 1.x and SAML 2.0 are supported.

**SPML**

For user provisioning. Using SPML users can be created and an external system notified, to trigger the provisioning of a user.
LDAP
LDAP V3 is supported as defined by rfc 510 - rfc 4519.

PKI
X.509 V3 certificates are supported as defined in rfc 5280.

Branding
Customers can specify logos, headers, color schemes and button colors in the Registration, Profile Management and Authentication screens.

Service Management

On-boarding
Verizon’s team of experts helps to provide a successful, efficient and trouble-free implementation. The integration of UIS into the customer environment can be viewed as three distinct stages, all managed and supported by Verizon Professional Services. Please refer to the UIS Statement of Work for a detailed description of these deliverables.

Discovery and Analysis
An in-depth discovery meeting is conducted to discuss the goals of the implementation, define specific technical challenges and ensure alignment on the business problems UIS is going to solve. This step also details the systems that will be integrated into UIS and the protocols and processes that will be employed between the customer’s environment and Verizon.

Planning
The planning stage focuses on integration and implementation planning and outlines all the steps of the process, identifying associated dependencies and proposing project timelines.

Deployment Campaign
The final stage, the Deployment Campaign, establishes how UIS will be launched in the customer’s environment, utilizing a phased approach to successful adoption within the user community. Typically this program is designed to roll-out UIS to an initial user group, a secondary release group and a final release to the entire user base.
Professional Services

UIS includes Verizon Professional Services for these three stages. The Statement of Work provides a detailed description of the deliverables.

Service Commencement

The service is considered to have started when the customer receives the credentials for the first administrator.

Service Termination

Once service has commenced, the service will run for 12 months after which either Verizon or customer may issue written notification of the termination of contract that will be effective at the end of the following complete month. At the termination of this service, Verizon will support the transfer of customer user and token registration files to the customer or their designated agent on a time and materials basis. Verizon retains ownership of any hardware tokens and of any user licenses.

If neither party terminates the service after the initial 12 months, the service will automatically renew for an additional 12 month term.

Service Levels

This service provides authentication services through an SLA-based delivery model. The SLA for this service offers high levels of availability 24/7/365 for its authentication services, user portal and administrative portal. All availability figures exclude scheduled maintenance windows. Availability is as determined by Verizon’s system monitoring structure. Terms and conditions apply; see your Verizon account manager for details.

Change Control

Changes to the service can be carried out by the UIS Service Management team. This team will work with customers to get additional users set up on the system. They can also facilitate additional applications support and supporting other customer needs such as obtaining additional form factors or tokens as needed.

Service Monitoring

Industry-standard monitoring tools are used to detect any problems with the service quickly and efficiently. Areas that are monitored include:

1. Infrastructure
2. Application
3. UIS Self Monitoring

4. Security

Extensive reporting is a crucial part of this service. Monthly services reports can be emailed to select Customer Administrators.

Reports are generated in the following areas:

- (Per Tier) Help Desk
  - Ticket volumes
  - Issue categories/volumes
  - Monitoring Triggered Events
  - Metrics
    - Priority
    - Time per call
    - Time per issue
    - Escalation metrics
      - Tier 1 to Tier 2
      - Tier 2 to Tier 3
      - Management
- Registration Authority (RA) Reporting
  - RA volumes by client
  - Metrics
    - Time per RA action
- Service Level Agreement (SLA) Reporting
  - By customer
  - Historical information
  - Trend reporting

Logging is also available upon request. Logs are written as flat files within the UIS environment and are accessible to customers through a trouble ticket. Log archiving and availability as well as specific log details can be defined on a per-customer basis.

Incident Handling

End-user Support - Tier 1

Tier 1 support is maintained by the customer and if the customer’s Helpdesk cannot solve a problem, they can escalate the issue to the Verizon UIS Helpdesk for Tier 2 support.

Tier 2 Support

Authorized customer help desk personnel can e-mail or phone the UIS Tier 2 Helpdesk to raise issues. The Helpdesk will issue a ticket with a severity level defined in the following table:
<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Problems which prohibit critical business operations in the customer’s production environment</td>
</tr>
<tr>
<td>2</td>
<td>Failure of one or more of the system functions making use of the system/service difficult</td>
</tr>
<tr>
<td>3</td>
<td>Failure of a system function having no significant immediate effect on the system/service operation.</td>
</tr>
<tr>
<td>4</td>
<td>Requests for information.</td>
</tr>
<tr>
<td>5</td>
<td>Requests for changes.</td>
</tr>
</tbody>
</table>

If an issue is not resolved within the average targeted timeframes, the customer may request that the issue is escalated. See table below:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Targeted Response Time</th>
<th>Target Resolution / Workaround Time</th>
<th>1st Escalation</th>
<th>2nd Escalation</th>
<th>Final Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15 minutes</td>
<td>1 hour</td>
<td>1 hour</td>
<td>2 hour</td>
<td>3 hours</td>
</tr>
<tr>
<td>2</td>
<td>Less than 1 hour</td>
<td>Less than 4 hours</td>
<td>1 hour</td>
<td>4 hours</td>
<td>24 hours</td>
</tr>
<tr>
<td>3</td>
<td>Less than 2 hours</td>
<td>Less than 40 hours</td>
<td>1 hour</td>
<td>24 hours</td>
<td>40 hours</td>
</tr>
<tr>
<td>4</td>
<td>Less than 8 hours</td>
<td>Less than 80 hours</td>
<td>2 hours</td>
<td>48 hours</td>
<td>60 hours</td>
</tr>
<tr>
<td>5</td>
<td>5 Business Days</td>
<td>TBN</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

As UIS may access services run by the customer (e.g. Active Directory) and provides services to other customer services (e.g. VPN service), issues may arise due to integration with such services. The customer is responsible for providing adequate and timely technical support so that investigations into such issues may proceed with urgency. If the customer fails to provide such support in an adequate and timely fashion then any consequent delays will be taken into account when calculating availability.

**Verizon Responsibilities**

Verizon provides a 24 x 7 two tier helpdesk as part of this service. The two tiers share the same Remedy ticket management system. Authorized customer support personnel have access to Verizon’s Remedy ticket management system allowing the customer to integrate UIS tickets with the customer’s own ticket management system. Tier One support is provided by the customer’s Helpdesk.

Tier 2 support is provided by Verizon UIS Helpdesk operators and can be called by authorized customer administrators to:

- Provide Level 2 End User technical support
- Reset incorrect passcode retry count
• Enable/disable tokens
• Provide emergency access to end users
• Reset PINs
• Reset passwords
• Re-synchronize tokens
• Replace failed or broken tokens (the customer will be charged for such replacements)
• Enable/disable accounts
• Terminate end user sessions
• Assisting users who have difficulty installing UIS-related software on smartphones
• Receive batch files for bulk management of end users
• Add or remove an Agent
• Add or remove Customer Administrators and Customer User and Token Administrators ("Customer Administrators").
• Receive incident reports

Tier 3 helpdesk operators will be engaged by Tier 2 as necessary at the application and server infrastructure level.

While the customer or their agents are responsible for configuring client services which utilize UIS for the authentication of users, Verizon will assist the customer with the testing of such services to confirm that the configuration works correctly. Similarly, if there are problems with client services authenticating users, Verizon will work with the customer to analyze the problem and, if the problem is found to be with the client service, assisting the customer with finding the solution to the problem.

**Security ServicesAdvisor**

UIS customers are assigned a Security Services Advisor ("SSA"). The SSA is a shared resource assigned to multiple customer accounts that will be responsible for providing the following services.

The SSA will host quarterly service review meetings to discuss one or more of the following items:
• Relevant service reporting and customer trends as demonstrated by these reports
• Major incidents requiring further discussion
• Planned customer activities for the next quarter
• Planned release and service features
• Service Level Agreement performance

The SSA also serves as the escalation point for,
• Questions about the extent of the services delivered within this agreement
• Quality of Service / Service Level Agreement enquiries

**Customer Responsibilities**

Verizon prefers for a client to designate a single point of contact ("SPOC") who will be responsible and authorized to:

(i) make all decisions and give all approvals which Verizon may need from Customer, and
(ii) provide Verizon’s personnel on a timely basis with all information, data, access and support reasonably required for its performance under the UIS Service Attachment, including but not limited to making available appropriate personnel to work with Verizon as Verizon may reasonably request.

Clients are also responsible for:

- Completing the enrollment form accurately and completely in the time period requested by Verizon.
- Designate the following Administrators:
  - Customer Administrators. In addition to performing actions permitted by User and Token Administrators, the Customer Administrator’s responsibilities include:
    - Completing the Enrollment Form.
    - Requesting the addition or removal of other Customer Administrators and tier 1 helpdesk operators.
    - Receiving monthly standard SLA reports.
    - Receiving a quarterly standard comprehensive log of all authentication and administration activity.
    - Receiving notification from Verizon by email or other mutually acceptable means of scheduled maintenance.
    - Submitting batch requests to the Administrative Console. The batch file can contain requests for adding and managing users including associating tokens with users. The format for the batch files is specified in the Universal Identity Services administrator guide.
    - Request changes (additions, removals and amendments) to Agents at Customer’s cost.
    - Receive incident reports problems including related to batch and Agent changes.

Security Controls

Separation of Data

Verizon utilizes strict security controls so that data on users and relying parties for one customer are not visible to administrators or users of another customer.

Data Protection

Verizon has a comprehensive data protection regime. This regime helps prevent unauthorized access to Customer data. This regime includes:

- Formal HR policies to confirm that Verizon employees are trustworthy.
- Formal policies on handling and safekeeping backups of customer data.
• Physical access control so that unauthorized persons may not access devices holding customer data.
• Network controls to help prevent unauthorized network access to customer data.

Network

UIS helps protect against network-based attacks using many techniques including:

• Firewalls
• Intrusion detection systems
• Sensitive customer information is not held on devices in DMZs.
• Protection against DoS and DDoS attacks.

Business Continuity and Disaster Recovery

UIS is based on web-services technology. All elements of the service are replicated at a primary production site to help prevent service outages. Production sites are fully equipped with dual Internet access and emergency power supplies.

To help protect against disasters affecting a primary production site, all elements of the service are replicated at a secondary site which is geographically remote from the primary site. Following a disaster, services will be rapidly switched to a secondary site.

Terms and Definitions

The following terms and abbreviations are used frequently in this document. This list is provided as a quick reference for your convenience. Acronyms/abbreviations that appear only once, or appear only in a small section of the test procedure, may be explained within the text and do not necessarily appear in this listing.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Authentication</td>
<td>A method of authenticating a user where the method employed can be varied to meet the requirements of the level of assurance or transaction risk.</td>
</tr>
<tr>
<td>Authentication Service</td>
<td>A service provided to a requesting service or target application that validates the credential or token as being in good standing.</td>
</tr>
<tr>
<td>Credential</td>
<td>See NIST definition.</td>
</tr>
<tr>
<td>DEA</td>
<td>Drug Enforcement Agency</td>
</tr>
<tr>
<td>Dispatched Notary</td>
<td>A notary sent to a user from an organization of professional notaries. This notary has all the appropriate identity forms and</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>handles the scheduling of the identity proofing visit.</td>
<td></td>
</tr>
<tr>
<td>FBCA</td>
<td>Federal Bridge Certification Authority</td>
</tr>
<tr>
<td>ICAM</td>
<td>Identity Credential and Access Management</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration (US Government)</td>
</tr>
<tr>
<td>Identity Verification Service</td>
<td>A component service of the system that manages the subject’s identity verification. Depending on the NIST security level, this may be as simple as creating a user name and password or as complex as in-person identity verification with biometrics collection.</td>
</tr>
<tr>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>Knowledge-based Assessment (KBA)</td>
<td>A quiz administered to a subject or applicant that is based on previously collected historical identity data. The data formulating the basis of the quiz may be provided by a trusted third party source or from an Enterprise Repository.</td>
</tr>
<tr>
<td>OATH</td>
<td>Open Authentication; an accepted standard</td>
</tr>
<tr>
<td>OTP</td>
<td>One Time Password</td>
</tr>
<tr>
<td>Requesting Service</td>
<td>A system or service that is programmatically making a request of another service to perform a task or function, such as Authentication.</td>
</tr>
<tr>
<td>Self-Service Notary</td>
<td>A notary that is sought out by the user with the intent of verifying identity-proofing data.</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service (i.e. a text message on a mobile device)</td>
</tr>
<tr>
<td>Target Application</td>
<td>A system that is relying on a service to perform a task or function, such as Authentication.</td>
</tr>
<tr>
<td>Token</td>
<td>See NIST definition.</td>
</tr>
<tr>
<td>Trusted Registration Agent (RA)</td>
<td>An agent recognized and trained to collect identity proofing data on behalf of the system or the relying customer. A Trusted Agent is bound to the system contractually.</td>
</tr>
<tr>
<td>User</td>
<td>Any person or agent that accesses the system through a Target Application or Requesting Service.</td>
</tr>
<tr>
<td>User Agreement</td>
<td>Credential provider agreement between a user and the credential service provider that mandates the actions and behaviors that the user can perform with the provided credential.</td>
</tr>
<tr>
<td>Verizon Customer Agreement</td>
<td>An agreement between Verizon and a relying customer for identity management service. This agreement may define service levels, degrees of assurance and any other terms relevant to the delivery of identity management service.</td>
</tr>
</tbody>
</table>
About Verizon Business
Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world’s most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today’s extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world’s largest businesses and governments—including 99 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.