Usher Mobile Identity Platform
Security Architecture
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Usher Mobile Identity Platform</td>
<td>2</td>
</tr>
<tr>
<td>Usher Security Architecture</td>
<td>3</td>
</tr>
<tr>
<td>Usher Mobile App</td>
<td>4</td>
</tr>
<tr>
<td>Secure Data Transmission</td>
<td>8</td>
</tr>
<tr>
<td>Usher Server</td>
<td>10</td>
</tr>
<tr>
<td>Usher Connectors</td>
<td>12</td>
</tr>
<tr>
<td>Conclusion</td>
<td>14</td>
</tr>
</tbody>
</table>
Introduction

People use their identities every single day – for conducting transactions, to prove who they are, to authorize payments, and even to log on to their computer workstations. An individual’s verified identity is the only trusted method that organizations can reliably employ for granting access to facilities and systems, rendering services, or selling products to their customers. To establish who they are, people use traditional forms of identity, such as keys, government issued documents (including driver’s licenses or passports), and passwords. However, physical forms of identity such as badges and key cards are easily lost, stolen, or counterfeited, while usernames and passwords can be easily cracked or phished. Research shows that there were close to 28M stolen identity documents in circulation in 2011, while 76% of data-breaches were caused by exploited passwords. The inherent weakness of physical IDs and passwords costs businesses hundreds of billions of dollars in losses, including damaged reputations and undermined public trust.

Clearly, traditional forms of identity are failing and a robust solution is urgently needed to prevent cybercrime and fraud. Usher is a revolutionary mobile identity platform that is designed to help governments, businesses, and organizations securely counter the growing wave of cybercrime. Usher Mobile Identity replaces traditional forms of identity with secure mobile identity, delivering biometric-caliber security to every application and business process across the enterprise.

- **Replace traditional forms of identity** – Plastic IDs, keys, or passwords are converted into mobile identity that contains all credentials on a person’s smart phone.

- **Ensure user identity** – Usher Mobile Identity can be biometrically linked to its owner, ensuring that only the true owner can activate their mobile identity and use it.

- **Use mobile identity in every business process** – Usher lets individuals use their mobile phones to validate identity, log on to applications or computer workstations, open entryways, and authorize transactions.

![Figure 1. Usher replaces physical forms of identity with mobile identity and extends it to every application and business process.](image-url)
Usher Mobile Identity Platform

The Usher Mobile Identity Platform’s three-layer architecture, with security features built into each layer, ensures that mobile identities are always secure, accurate, and valid.

The Usher Mobile Identity Platform consists of three components:

- **Usher Mobile App** – An elegant and powerful mobile app that allows people to validate identities or conduct transactions. The mobile app stores only a simple descriptive portion of the user’s identity, using time sensitive codes to verify or share identity.

- **Usher Server** – A high performance, scalable, and secure system that synchronizes identities with Enterprise Identity Management systems (IDMs) of record. The Usher Server accesses ID repositories through connectors and presents identities to Usher Clients.

- **Usher Connectors** – Individual connectors, through which the Usher Server sends and receives verified identities with Identity Management Systems, ensure that the IDMs are never directly exposed to external Usher or non-Usher Clients.

![Diagram of Usher Identity Platform](image)

Figure 2. The Usher Identity Platform’s three-layer architecture ensures that mobile identities are always secure and valid.

The security features built into each layer of the Usher Identity Platform are synchronized to ensure that an individual’s mobile identity always stays secure and is extremely difficult to compromise.
Usher Security Architecture

This section will focus on 14 distinct security features that are built into the three-layered Usher Security Architecture and the communication protocol that the Usher Server, Usher Clients, and Usher Connectors employ for data transmissions. While each individual security feature performs an important function to keep the system and mobile identity data secure, the combination of these features together ensures that the Usher Platform provides the highest level of security to organizations and users against fraud, cybercrime, and brute force attacks.

Figure 3. Powerful security controls built into the Usher Identity Platform ensure that it provides the highest levels of security to users.

The next few sections discuss the architectural design of these security controls that are built into the layers of the Usher Mobile Identity Platform.
**Usher Mobile App**

Locally on the mobile phone, the Usher Mobile App stores nothing more than basic user information, an access token that authenticates the user, and a X.509 certificate that identifies the smart phone to the Usher Server as an Usher-enabled device.

Only a simple, descriptive part of the identity is stored on the phone.

- **User attributes**
  - John Doe
  - Product Manager
  - Name Software, Inc.

- **Picture**
  - A photo of the user for visual identification

- **X.509 certificates**
  - An X.509 certificate ensures that only Usher Identities are authenticated

- **Access token**
  - An access token for authentication of the user

**Figure 4.** The Usher Mobile App stores data on the smartphone in an encrypted format.

**Security feature 1: 256-bit encryption of user attributes**

Only basic identity information, such as a user’s name, title, company, and photo, is stored locally on the client. All user attributes are encrypted with 256-bit AES encryption and stored in the phone’s encrypted storage area, ensuring that the user’s data is extremely difficult to compromise.

**Figure 5.** Basic user information is stored in an encrypted format on the smartphone.
Security feature 2: Integrated with biometrics

Biometric capabilities built into Usher Mobile App ensure that only the true owner can use their mobile identity. Various biometric modalities (voice, facial) are used for identity verification, while sophisticated algorithms are integrated into the security architecture to precisely detect fraudulent techniques (recorded sounds or pictures), ensuring that mobile identity is always secure. Biometric verification can be tied to any authentication event or any number of workflows, including physical and logical access, identification, high-risk transactions, among others. This prevents unauthorized use of the mobile identity and provides an additional authentication factor for highly secure situations.

With voice biometrics, the Usher user recites a dynamic code displayed on the phone screen, then the Usher Server matches the voice print with the voice print database and, upon a positive match, releases the mobile identity for authentication. With facial biometrics, the Usher Mobile App scans the user’s face while the Usher Server matches it with the face print database and, upon a positive match, releases the mobile identity for external actions.

Figure 6a. Usher’s integration with voice biometrics prevents unauthorized use of mobile identity.

Figure 6b. Usher’s integration with face biometrics prevents unauthorized use of mobile identity.
**Security feature 3: Encrypted access tokens for authentication**

Usher employs access tokens instead of user names and passwords for user authentication, eliminating the need to send user credentials over Wi-Fi, 3G or 4G networks for user authentication. This ensures that credentials cannot be intercepted or phished during data transmission. Access tokens are stored in an encrypted format on the mobile phone and are only valid for a specific, configurable time period. Upon expiration, Usher users must re-authenticate themselves to the Usher Server and obtain a new token.

![Image of Usher mobile app with encrypted access tokens](image_url)

*Figure 7. Usher employs encrypted access tokens to authenticate users preventing user credentials from being stolen and phished over Wi-Fi, 3G or 4G wireless networks.*

**Security feature 4: Time-limited Usher Codes**

Usher users enter time-limited Usher Codes into their Usher Mobile App to verify the identity of other users. These Usher Codes are time-bound, valid only for a pre-set, configurable time period, with a default setting of 30 seconds. Usher Codes include a QR Code and the numeric Usher Code. After the pre-set time period expires, each Code is refreshed and replaced with a newly generated Code. The previous code is rendered invalid and can no longer be used. All Usher Codes are linked to a specific device enabling the Usher Server to precisely identify the device being used. This architectural design ensures that the security risk associated with stolen Usher Codes is minimal, preventing replay attacks. Given the time sensitivity, these codes are designed to withstand brute force attacks. In short, the attacker only has the time period for which the Usher Code is valid to try each and every combination, making it highly improbable for the in-use Usher Code to be guessed.
Security feature 5: Offline Usher Code generation

All Usher Codes used for identification are generated on the client, including the QR Code, numeric Usher Code, and Sight Code. For numeric Usher Code generation, the Usher Server sends an initial key to the Usher-enabled device, which stores this key on the phone in an encrypted format. The Usher-enabled device then uses this key to generate time-limited numeric codes locally on the smartphone. The Usher Architecture is designed such that the initial key remains valid only for a specific time period (24 hours). Upon expiration, the Usher Server issues a new key to the device for generating a new set of codes. The time-limited codes are not only designed to withstand brute force attacks but also make it highly improbable for the code to be guessed. In addition, the Usher Server will throttle any attempts to guess Usher Codes, thereby preventing an attack.

Figure 8. One-time, time-limited Usher Codes act as short-lived, temporary identifiers of the client.

Figure 9. Usher generates time-limited codes on the client.
Security feature 6: Encrypted X.509 certificates for all Usher-enabled mobile devices

Usher uses X.509 client certificates to help secure communications between the Usher Mobile App and the Usher Server. The Usher Server issues a unique X.509 certificate to each Usher-enabled device when the Usher Mobile App is launched for the first time on that device. This certificate is generated to the X.509 SSL standard and, upon issue, is stored in the mobile phone's encrypted storage area. A mobile phone identifies itself as an Usher-enabled device to the Usher Server by including its unique X.509 certificate in every data transmission, thus preventing rogue devices from impersonating an Usher device and establishing fraudulent communication with the Usher Server to steal identity information.

Figure 10. Usher Clients employ 256-bit AES encryption for storing a X.509 certificate.

Secure Data Transmission

Usher Clients, Usher Server and Identity Management solutions use Secure Sockets Layer (SSL) protocols to securely exchange identities and communicate with each other.

Security feature 7: Out-of-band Identity transmission

All identity information is transmitted out-of-band from the Usher Server to the Usher Mobile App. This ensures that no two Usher clients directly share identity data and that the identity is always validated independently by the Usher Server. This includes identity validation through QR and numeric Usher Codes. This approach also ensures that malicious apps can never steal identity data from the smart-phone client. Additionally, since a malicious app cannot present a valid Usher issued X.509 certificate, the Usher Server will immediately reject any communication attempts from it, ensuring that identities always remain secure.
Security feature 8: Encrypted channel for data transmissions uses SSL protocols with X.509 certificates

Usher Clients, Usher Server, and the underlying Identity Management Solutions use 256-bit SSL protocol to send identity verification requests and verified identities to another. These requests include the access token for user authentication, the X.509 certificate to identify the device, an Usher Code, and the requested transmission is always encrypted. The Usher Server matches the client X.509 certificate with a copy maintained in the Usher Server database and, upon positive match, sends the verified identity back to the client. This process ensures that only known Usher-enabled devices can send identity requests to the Usher Server and receive identity information from it. Additionally, all identity requests are processed exclusively through the Usher Server which, in turn, accesses identity information through Usher Connectors.

SSL pinning: To ensure that the client is talking only to known servers, all trusted servers’ certificates are pinned in the application to prevent a man-in-the-middle attack that may use fraudulent certificates or malicious proxy servers. The usage of SSL pinning also prevents cyber thieves from deploying a fraudulent server to masquerade as an Usher Server.

Figure 11. Identity information is always transmitted out-of-band from the Usher Server to valid Usher Clients.

Figure 12. Data transmitted by Usher Clients includes a X.509 certificate and is encrypted using SSL protocols.
**Usher Server**

The Usher Server is a high performance, scalable, and highly secure system that interacts with Usher Clients and Identity Management Solutions. The Usher Server receives verification requests from the client, makes requests of the Usher Connectors to fetch identities by accessing the Identity Management Solution repositories, and delivers verified identities to Usher Clients through out-of-band communication. Security features are built into the Usher Server to ensure that malware, rogue apps, or hacking attacks cannot steal identity information. This architectural design lets the Usher Server provide single sign-on functionality for all SAML 2.0, OpenID Connect, and OAuth 2.0 compliant web applications.

**Security feature 9: Encrypted X.509 certificates on the Usher Server**

The Usher Server maintains an encrypted copy of each client certificate it signs and issues, using the certificate to bind a user and a device. This stored certificate is used to verify each server request from the client, ensuring that all server requests are coming from a valid device and an authorized Usher user.

![Usher Server Diagram](image)

*Figure 13. The Usher Server maintains an encrypted copy of each Usher Client’s X.509 certificate in its database.*

**Security feature 10: The Usher Server is the sole Certificate Authority**

The Usher Server Architecture is built on Public Key Infrastructure (PKI) to ensure that only authorized Usher users communicate with the Usher Server, and only from authorized Usher Client devices. The Usher Server has the sole authority to convert a mobile device into an Usher-enabled device by granting it a signed client certificate. This process ensures that rogue devices or applications cannot masquerade as Usher-authorized devices by presenting unknown certificates to Usher Server.
When the Usher app is launched for the first time, the client generates a certificate signing request (CSR) and sends it to the Usher Server. This client-generated CSR includes standard information such as domain and organization name and it is signed with the client’s private key. The CSR also includes the client’s public key. The Usher Server generates and signs a X.509 digital certificate, saves a copy of this certificate in its database, and returns the signed certificate to the device. As soon as the client receives the signed certificate, it encrypts the certificate and stores it securely on the client. From this point on, the client includes its own signed certificate in every server request; and the Usher Server matches the client certificate with the copy from its own database to ensure that every request is made by a legitimate Usher-enabled device.

![Diagram of certificate process]

Security feature 11: Fully compliant with OAuth 2.0 standards

The Usher Mobile Identity Platform Architecture is built using OAuth 2.0 standards, an open standard for authentication and authorization, incorporating the following characteristics:

- The Usher Server includes an authorization layer to grant or revoke X.509 certificates.
- The Usher Server uses access tokens to authenticate users, instead of their usernames and passwords.
- The Usher Server is the “Registration Authority” which, upon successfully verifying the identity of a user, registers the user in its database and issues an access token.
- First-time user authentication can be achieved out-of-band, such as sending an authorization code to a registered email, which can then be used to complete the registration process.
Security feature 12: Caching of user attributes in an encrypted format

The Usher Server securely caches user attributes received from the underlying Identity Management Solutions (IDM) in an encrypted format, improving overall performance by eliminating the need to continuously pull data from the IDM on every request. The data cached is minimal and includes basic user description attributes. The full identity is never stored on the Usher Server, ensuring that the identity is always protected.

Usher Connectors

Individual connectors, through which the Usher Server sends and receives verified identities with Identity Management Systems, ensure that the IDMs are never directly exposed to external Usher or non-Usher Client requests.

Security feature 13: Connectors for Identity Management System

The Usher Server uses secure connectors to communicate with user repositories hosted in IDMs and in physical access control systems (PACS). Each connector is integrated with the Usher Server and the Usher Server and Identity Management System use an independent connector access token to authenticate themselves. This eliminates the need to send user credentials for accessing the Identity Management System. Read-only accounts are used to access the IDM ensuring that no user information or user permissions will be overwritten. Out-of-the-box, the Usher platform supports databases, LDAP, OpenLDAP, Active Directory, IBM Tivoli, and Oracle Identity Management IDMs and supports Lenel, S2, Honeywell, Mobotix, and Data Watch physical access control systems. The Usher Server’s communication through bi-directional connectors ensures that the identities stored in the IDMs are never directly exposed to external applications or devices, preventing identity theft and fraud.
Connector for Identity Exchange

1. Individual connectors for each Identity Management Solution
2. Server and connectors authenticate with a connector access token
3. Each connector is integrated with the Usher Server
4. Supported Identity Management Solutions include:
   - Active Directory and LDAP
   - Database
   - Oracle Identity Management
   - IBM Tivoli

Figure 16. Usher’s bi-directional connectors ensure that the IDM solution is never exposed to external attacks.

Security feature 14: Encrypted X.509 certificates for each Identity Management System

The Usher Server maintains an individual, encrypted client certificate for each connected IDM solution with which Usher communicates. Each X.509 certificate is generated by the Usher Server only once and is stored on the Usher connector, thereby uniquely identifying the IDM to the Usher Server. A corresponding copy of the certificate is stored in an encrypted format in the Usher Server’s certificate database. This architecture is designed to prevent a fraudulent Usher Server from communicating with Usher Connectors and stealing identities, defending the system against cybercrime and fraud.

Figure 17. Encrypted X.509 certificates for each connected Identity Management System.
Conclusion

The Usher Mobile Identity Platform is designed for enterprises and organizations to dramatically lower fraud and improve the cyber security of every business process in their operations. The Usher Identity Platform’s three layer architecture, with security features built into each layer, provides robust security against identity theft and cybercrime. While each security feature is independently designed to protect an individual’s mobile identity, all of the security features work together to ensure that Usher Mobile Identity remains highly secure and available. Biometric capabilities ensure that only the true owner can use their Usher Identity for transactions, payments, accessing buildings and facilities, or to safely log on to web applications and computer systems. Usher Mobile Identity provides organizations and enterprises a convenient, reliable, and secure alternative to protect sensitive data and intellectual property, mitigating the threat of cybercrime.