ZEBRA

Identity Guardian

Simple and Secure Mobile Device Authentication

Table of Contents

Simple and Secure Mobile Device Authentication

Identity Guardian offers secure, personalized access to mobile devices and applications for both shared and personally assigned device deployments. Leveraging facial biometrics and multifactor login, it protects personal information and corporate data while providing a seamless and efficient sign-in experience.

Key Features and Benefits

Facial Biometrics: Effortlessly and securely unlock mobile devices with the same ease as personal cellphones. This enhances the user experience by providing a familiar and quick authentication method.

Multifactor Authentication: Enhance security by employing multiple authentication factors for device access, minimizing the risk of unauthorized access and theft.

Accountability and Visibility: Administrators gain comprehensive visibility into device usage and associated users, tracking device sign-ons and sign-outs through the Zebra DNA™ Cloud platform.

Simplified Application Authentication: Integration with identity providers (IdPs) enables single sign-on (SSO), streamlining the login process which can help seamlessly log in to other app on the device and reducing user frustration.

Personal Data Protection: Multiple layers of security safeguard employees' personal data on both shared and personally assigned devices.

Personalization: Create unique, role-based user experiences on devices, tailoring the interface to meet specific user needs and improving overall efficiency.

Enablement via API: Allow other applications installed on the device to interact with and gather information from Identity Guardian, providing opportunity for integrated workflows, and more.

In today's rapidly evolving digital landscape, where data breaches and unauthorized access pose significant threats, Identity Guardian provides a dependable and effective solution. It strengthens your security measures and boosts user productivity by minimizing time spent on repetitive logins. This innovative tool seamlessly integrates into your existing systems, providing advanced yet user-friendly security.

System Overview

Frictionless Authentication

Identity Guardian is a cutting-edge solution offering convenient and secure user login for both shared and personally assigned enterprise mobile devices, ensuring top-tier protection and privacy for user and corporate data.

User Enrollment

Creation of User Barcode: During enrollment, a user barcode is generated based on the entered user data and captured face vectors. This data is encrypted using the Customer public key before being stored in the barcode.

- **User Authentication:** Authentication can use one or more factors, such as a scheme that includes only facial recognition.
- **Authentication would involve:**
  - **Scan User Barcode:** The barcode containing the encrypted data is scanned and decrypted with the Customer private key
  - **Capture Facial Vector Data:** The user captures their facial vector data live using the camera

Share Mode

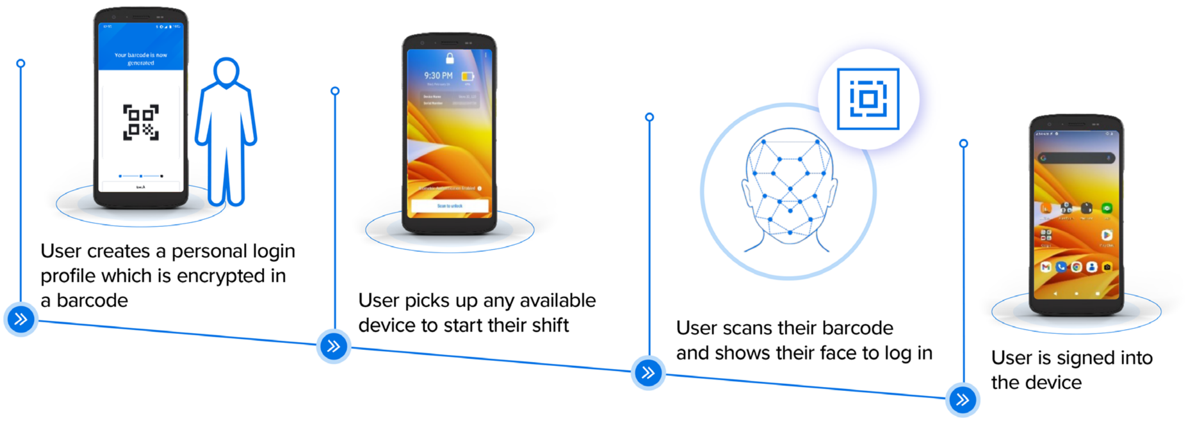
Identity Guardian is perfectly tailored for shared environments, ensuring smooth integration without compromising security. Scalability is limitless, enabling every enterprise device to recognize each user seamlessly.

Personal Mode

Identity Guardian seamlessly adapts to personally assigned mobile devices, providing a hassle-free setup for individual users akin to using a personal cellphone.

But similarities end there. Identity Guardian surpasses standard consumer solutions by providing advanced professional capabilities.

Shared



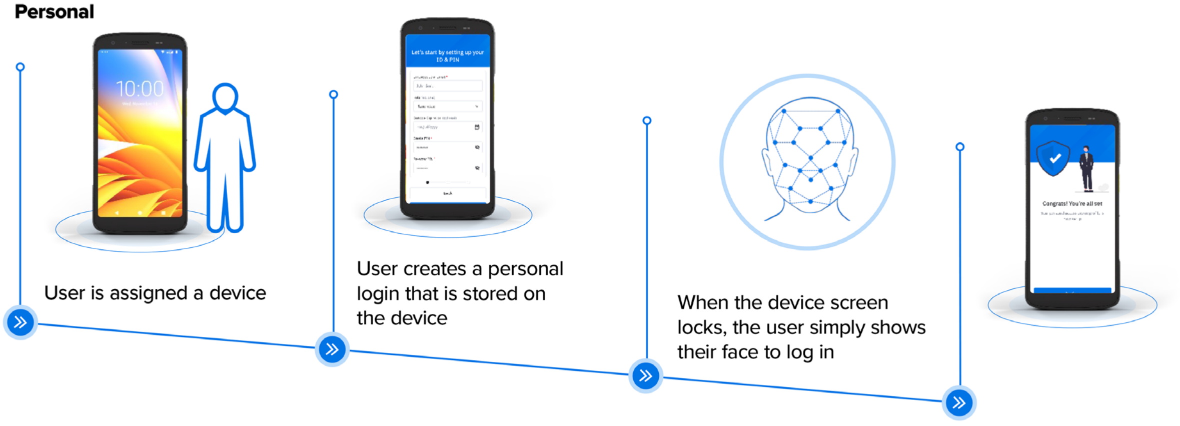
User creates a personal login profile which is encrypted in a barcode

User picks up any available device to start their shift

User scans their barcode and shows their face to log in

User is signed into the device

Personal



User is assigned a device

User creates a personal login that is stored on the device

When the device screen locks, the user simply shows their face to log in

Face Authentication

Identity Guardian allows the user to log in to the device using Face Authentication.
The complete process involved two phases:

- **Enrollment**: The process of capturing users' facial vectors and storing on a barcode.
- **Authentication**: The process of authentication of user using the data stored on the barcode and comparing with the users face vectors.

The live-captured facial vector data is compared to the data stored in the barcode. If the data matches, the device is either unlocked or advances to the next level of authentication as configured by the administrator.

This combination of AES-128 and RSA-2048 provides an enhanced level of security. Even if a hacker were to obtain the encrypted facial data stored on the barcode, they would not be able to decrypt it to identify the person behind that data, as they would not have access to the private key.

Note: For true 2-factor authentication, add a PIN or SSO in addition to the facial vector comparison.

Liveness Detection

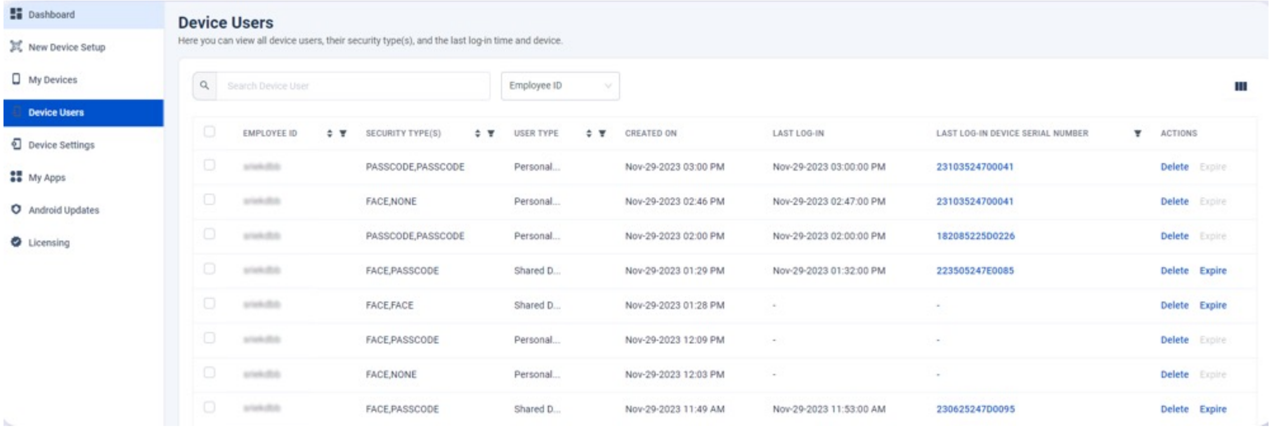
The AI-based liveness detection algorithm differentiates between genuine human features (such as a real iris or face) and fraudulent attempts (such as spoof attacks using masks, photos, or videos). There are three basic methods for liveness detection:

- **Active Liveness Detection:** Requires user actions, such as moving or turning their head. This method can be inconvenient and time-consuming.
- **Passive Liveness Detection:** Requires no user interaction, capturing only a single frame. This method provides a quick (1-2 seconds) and highly secure user experience.
- **Hybrid Liveness Detection:** Combines passive detection with minimal user interaction, such as asking the user to smile, offering maximum liveness security.

Identity Guardian uses the Passive Liveness Detection algorithm powered by a deep neural network, which analyzes parameters such as micro movements and light/shadow variations.

Admin Functionality

Leveraging the Zebra DNA Cloud platform, Identity Guardian provides administrators with complete visibility into user activities, allowing them to monitor device sign-ins and sign-outs, review security settings and more. Additionally, admins can manage barcodes by expiring or deleting them directly from the console.



Device Users

Here you can view all device users, their security type(s), and the last log-in time and device.

Search Device User | Employee ID

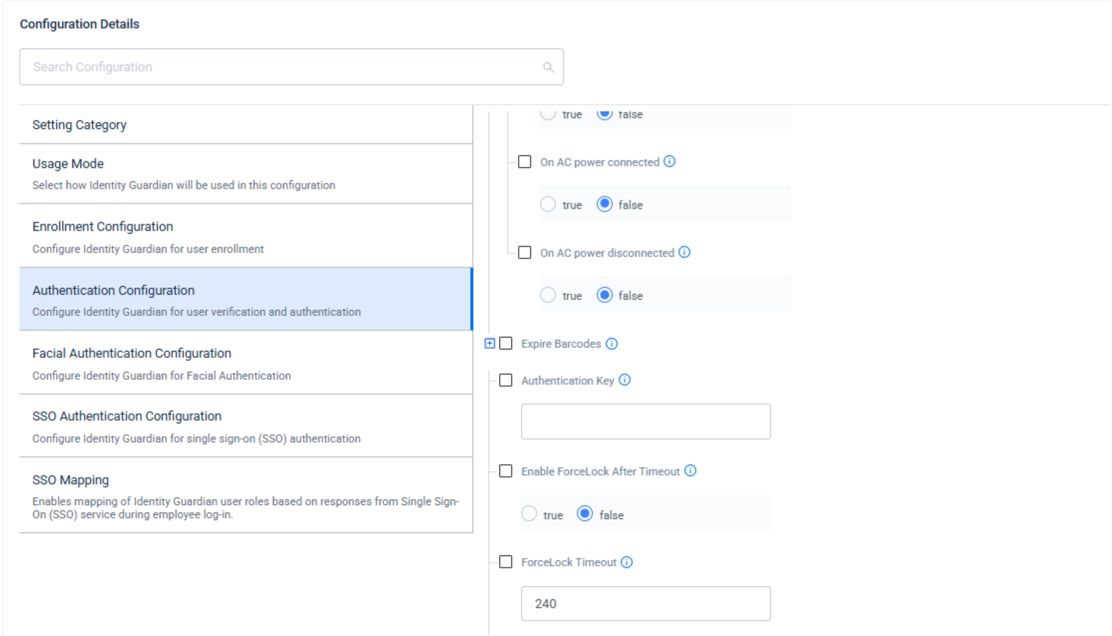
□	EMPLOYEE ID	SECURITY TYPE(S)	USER TYPE	CREATED ON	LAST LOG-IN	LAST LOG-IN DEVICE SERIAL NUMBER	ACTIONS
□	[redacted]	PASSCODE,PASSCODE	Personal...	Nov-29-2023 03:00 PM	Nov-29-2023 03:00:00 PM	23103524700041	Delete Expire
□	[redacted]	FACE,NONE	Personal...	Nov-29-2023 02:46 PM	Nov-29-2023 02:47:00 PM	23103524700041	Delete Expire
□	[redacted]	PASSCODE,PASSCODE	Personal...	Nov-29-2023 02:00 PM	Nov-29-2023 02:00:00 PM	182085225D0226	Delete Expire
□	[redacted]	FACE,PASSCODE	Shared D...	Nov-29-2023 01:29 PM	Nov-29-2023 01:32:00 PM	223505247E0085	Delete Expire
□	[redacted]	FACE,FACE	Shared D...	Nov-29-2023 01:28 PM	-	-	Delete Expire
□	[redacted]	FACE,PASSCODE	Personal...	Nov-29-2023 12:09 PM	-	-	Delete Expire
□	[redacted]	FACE,NONE	Personal...	Nov-29-2023 12:03 PM	-	-	Delete Expire
□	[redacted]	FACE,PASSCODE	Shared D...	Nov-29-2023 11:49 AM	Nov-29-2023 11:53:00 AM	230625247D0095	Delete Expire

Guardian Safe

Guardian Safe allows Identity Guardian to securely store unique application and website credentials in the cloud, ensuring users do not have to manually enter them each time they use a device. Identity Guardian remembers the credentials and automatically fills in the fields, streamlining access and enhancing user convenience.

Configurability

With Managed Configurations, Identity Guardian offers a comprehensive suite of options that enable customers to tailor the end user application experience according to their business requirements. From user profile creation to the initial and subsequent device sign-ins, every detail can be configured to ensure a seamless and secure experience.



Configuration Details

Search Configuration

Setting Category

Usage Mode
Select how Identity Guardian will be used in this configuration

Enrollment Configuration
Configure Identity Guardian for user enrollment

Authentication Configuration
Configure Identity Guardian for user verification and authentication

Facial Authentication Configuration
Configure Identity Guardian for Facial Authentication

SSO Authentication Configuration
Configure Identity Guardian for single sign-on (SSO) authentication

SSO Mapping
Enables mapping of Identity Guardian user roles based on responses from Single Sign-On (SSO) service during employee log-in.

○ true ● false

□ On AC power connected

○ true ● false

□ On AC power disconnected

○ true ● false

□ Expire Barcodes

□ Authentication Key

□ Enable ForceLock After Timeout

○ true ● false

□ ForceLock Timeout

240

Security

Data Storage

Identity Guardian implements multiple layers of protection to safeguard employees' personal data. The system specifically avoids storing sensitive personal data, such as facial vector data, on the cloud to mitigate liability concerns.

- **Shared Devices:** Employee personal data is securely encrypted within a personally managed barcode.
- **Personally Assigned Devices:** Employee personal data protection is handled within the Android™ framework, allowing employees to control and delete their personal data at any time.

For organizations where users need to log into multiple applications individually, Identity Guardian offers an optional feature that simplifies the process. It automatically fills in user credentials after verifying the user through a facial biometric scan or passcode entry. These credentials are securely stored in the cloud, enhancing user productivity, reducing errors, and streamlining the application login process. This feature requires the use of Identity Guardian with Zebra DNA Cloud.
This can be used by organizations where users need to log into multiple applications individually.

The following sections discuss the various scenarios in which data is secured.

Security of Data at Rest

Barcode data Encryption—Performed during User Enrollment

Step 1: Users perform Enrollment by providing the various user information.

Step 2: A random 128-bit AES Key is generated.

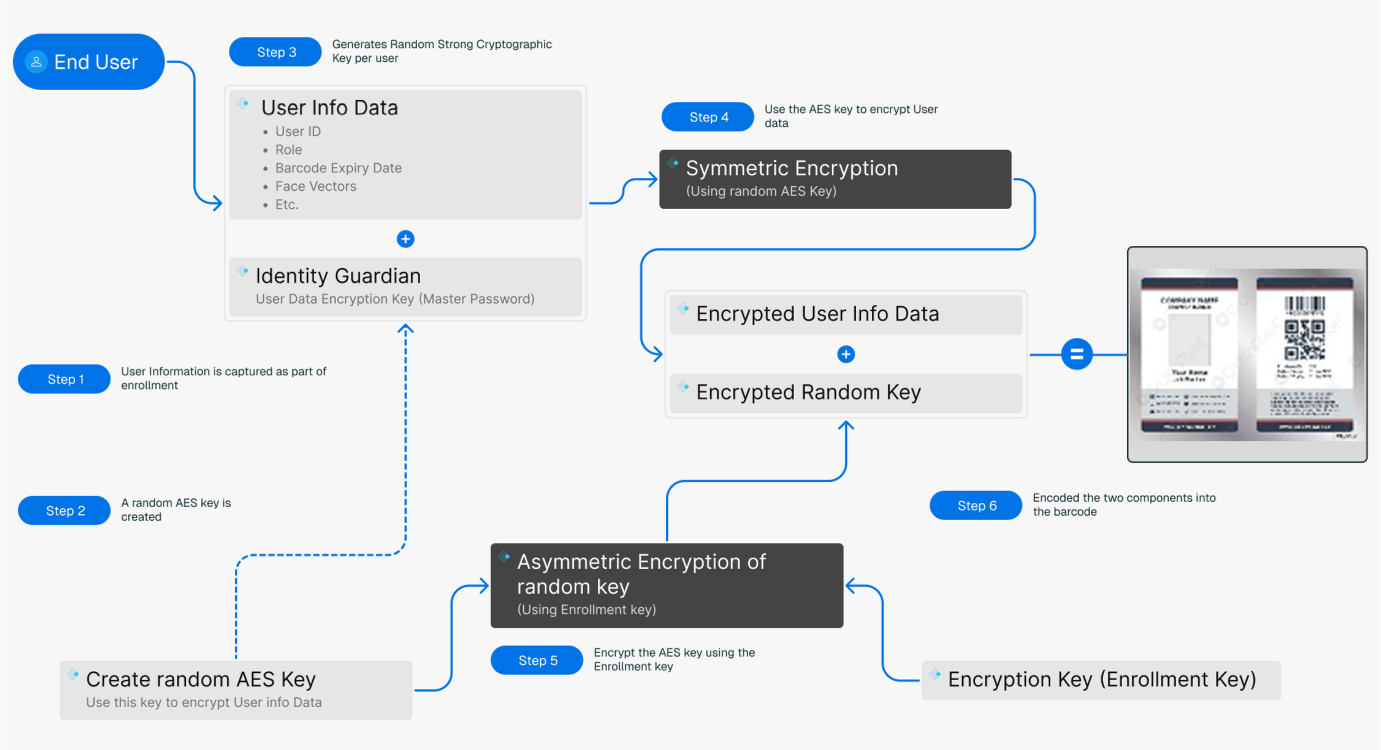
Step 3: An additional random 256-bit per User Key is generated referred to as Master Password. This key is used in Guardian Safe feature (explained further below), this key is appended to the captured user information.

Step 4: User information is encrypted using the randomly generated 128-bit key.

Step 5: The 128-bit key is encrypted by using the Admin provisioned Enrollment Key.

Step 6: The cipher text obtained in step 4, 5 are appended to create a master cipher text, this text is encoded into the barcode.

The diagram below highlights this flow:


End User
Step 3
Generates Random Strong Cryptographic Key per user
User Info Data
User ID
Role
Barcode Expiry Date
Face Vectors
Etc.
+
Identity Guardian
User Data Encryption Key (Master Password)
Step 4
Use the AES key to encrypt User data
Symmetric Encryption
(Using random AES Key)
Encrypted User Info Data
+
Encrypted Random Key
=
Step 1
User Information is captured as part of enrollment
Step 2
A random AES key is created
Step 6
Encoded the two components into the barcode
Asymmetric Encryption of random key
(Using Enrollment key)
Step 5
Encrypt the AES key using the Enrollment key
Create random AES Key
Use this key to encrypt User info Data
Encryption Key (Enrollment Key)

Barcode Data Decryption—Performed During User Authentication

When user scans the encrypted barcode, the cipher text is decrypted using the following process

Step 1: The payload is split into encrypted AES Key and encrypted user data.

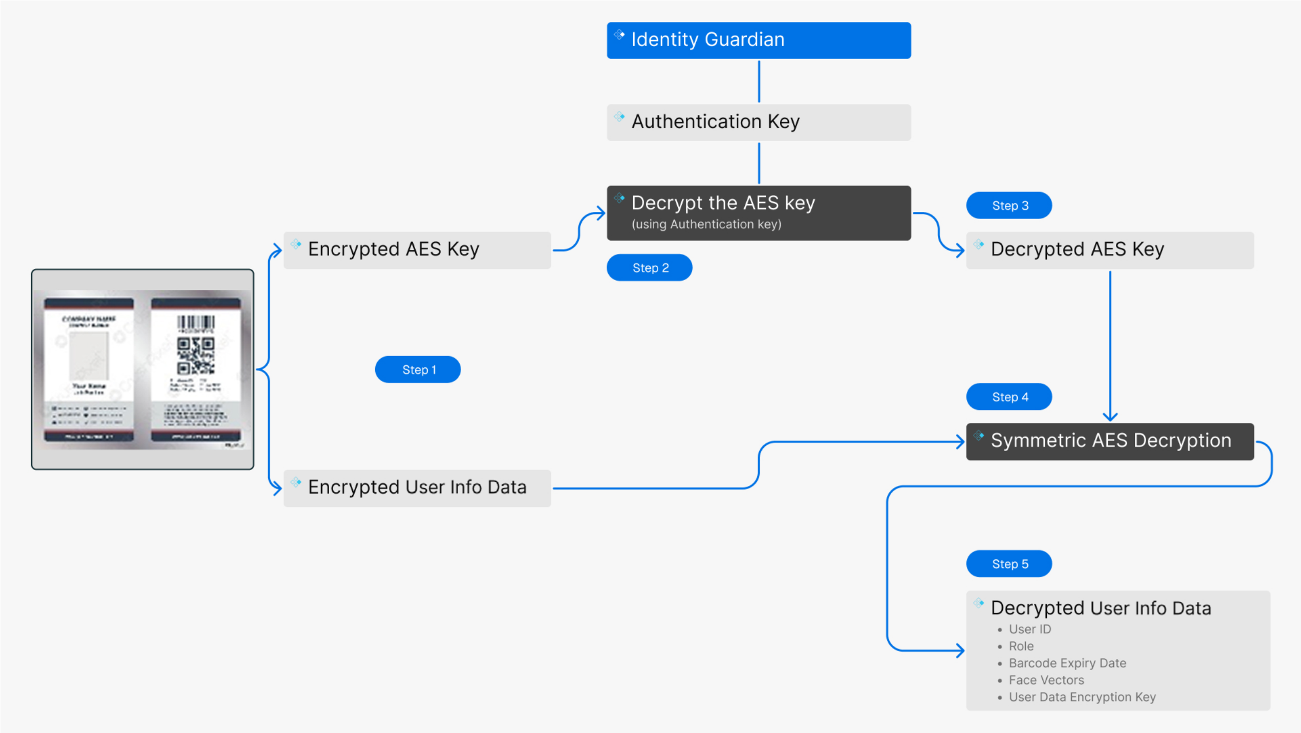
Step 2: The first part is decrypted to obtain the AES Key using the user provided Authentication Key.

Step 3: The AES Key is obtained.

Step 4: The AES Key is used to decrypt the user information.

Step 5: The user information is obtained.

The diagram below highlights this flow:



Data Stored on Device

Temporary storage of data

It is possible to store data temporarily when you scan a barcode. This data is stored on the device until either the user logs off or the session times out. This means whenever the user is done using the device and a new user picks up a device the data is deleted. This data is stored in Encrypted Shared Preference, which encrypts the data and then stores it in the application database. This allows the data to be safe even when the device is compromised.

Personally enabled

When IG is set in personally enabled mode, the user is not required to scan his barcode instead the enrollment data is stored within Identity Guardian. This data is stored in Encrypted Shared Preference, which encrypts the data and then stores in the application database. This allows the data to be safe even when the device is compromised.

Customer Enrollment and Authentication Keys

Identity Guardian uses the enrollment key and the authentication key. Ordinarily a device will not have both the keys if the device is set in enrollment mode, then it will have the encryption key and if the device is set in authentication mode it will have the decryption key. These keys are first encrypted on the server side using a Zebra proprietary desktop encryption tool and then sent to the device, where they are decrypted using Zebra proprietary secure storage. The secure storage is outside of Identity Guardian. Identity Guardian is whitelisted as a trusted application, which allows it to utilize secure storage and decrypt these keys. These keys are used on demand and are never stored in plaintext anywhere on the device.

PDF File

The enrollment barcode is stored as a PDF file on the device. This file is deleted after 24—32 hours.

Guardian Safe Data

Password vault data is triple encrypted: once by using customer-specific key, second by using a tenant-specific key, and the third by using a database-specific key. A detailed diagram of this process can be found in the document further down. When the password vault data is received on the device, this data is temporarily cached in encrypted shared preference and is deleted as soon as the user logs off.

Data Stored on Cloud

Guardian Safe data is stored on the cloud. The diagram below explains the setup and the security measures in place.

1. The user password is entered on the device using the Guardian Safe tool. This data is encrypted with the Master Password (AES-256) reffered as User Data Encryption in the diagram below, and an admin-provisioned Authentication Key (RSA-2048)

2.The data (encrypted blob) is passed to the Zebra DNA client on the device. The Zebra DNA client checks the signature and package name of the Identity Guardian application (first level of encryption).

3. The Zebra DNA client uploads the data to the Zebra DNA server via a secure connection.

4. The blob is received by the Password Vault Cloud Function, where it performs necessary permission and tenant checks to determine the appropriate tenant-specific database.

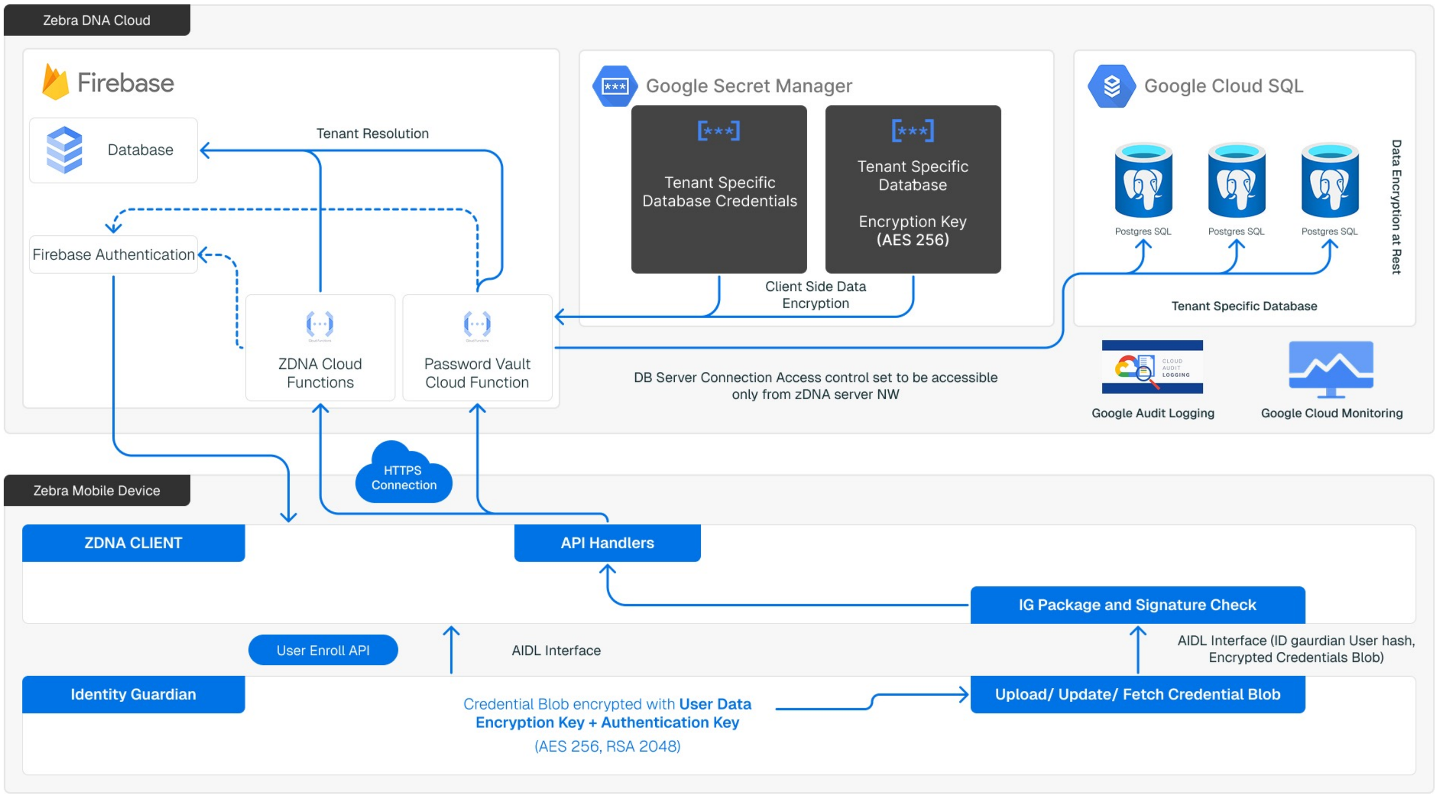
5. Once tenant details are obtained, the Password Vault Cloud Function accesses the tenant-specific database credentials and a tenant-specific Encryption Key.

6. The Encrypted Blob is then further encrypted using this tenant-specific Encryption Key (second level of encryption).

7. The Double Encrypted Blob is then stored in tenant-specific database.

8. This database server encrypts all the data at rest. This functionality is provided by Google (third level of encryption).

Data is fetched in similar manner by performing multiple levels of decryption.



Data Transmission

- **Data transmitted to Zebra DNA Cloud**
  - All data transmitted from mobile device to server is encrypted and transmitted over a minimum TLS 1.2 connection
  - Communications protocol is a mix of HTTPS and gRPC
  - The communication is bidirectional and data from the server to the device, and vice versa, is transmitted over the same channel
- **Managed config Security (cloud to device)**
  - Managed Configs are settings that are sent from EMM to the device; these configurations dictate how the application behaves. Some examples of configurations are if the Identity Guardian will operate in Enrollment or Authentication mode. The managed configurations are listed here https://techdocs.zebra.com/identityguardian/1-7/mc/
  - Some sensitive configurations require further securing, namely:
    - Enrollment Key: This is the public key of the RSA Key pair, used to encrypt the Barcode data during enrollment.
    - Authentication Key: This is the private key of the RSA Key pair, used to decrypt the Barcode data during authentication.
  - Both keys should be encrypted using a Desktop encryption tool on the computer, and the encrypted blob can be sent to the device via the managed configuration. The Decryption Key for these encrypted blobs can be accessed only by Zebra proprietary Secure Store Manager. This Secure Store Manager helps Identity Guardian decrypt the blobs and obtain the required keys.
  - The keys are never stored in Identity Guardian in plaintext format.

Device API Security

All Identity Guardian device side APIs are access controlled by package name and signature check for third party applications and Zebra signature check for Zebra applications.

Identity Guardian APIs can be called by any Zebra application signed by Zebra Keys.

If any third party or customer application wants to call Identity Guardian APIs, Admin must provide access to those APIs, allow listing the Package Name and signature of the customer application via Zebra Access Manager CSP. For more details, please refer to the following documentation https://techdocs.zebra.com/identityguardian/1-7/api/#requirements

Security Measures and Audits

Innovatrics, the provider of the Liveness Algorithm, has had its passive liveness algorithm independently audited by iBeta, an independent U.S. auditor. The algorithm has been verified to comply with ISO 30107-3 standards, which pertain to Level 2 Presentation Attack Detection (PAD).

For more information, refer to the ISO 30107-3 PAD Test Methodology and Confirmation Letter:

- iBeta ISO 30107-3 Presentation Attack Detection Confirmation Letters
- Innovatrics PAD Level 2 Confirmation Letter

Zebra's PEN testing methods and measures include Identity Guardian parameter settings and test results, ensuring a comprehensive evaluation.

By adopting Identity Guardian, organizations can enhance security and provide their workforce with a smoother user experience. This dual focus makes Identity Guardian a crucial tool for enterprises aiming to protect their most valuable assets: data and people. Empower your workforce to perform tasks efficiently and securely with Identity Guardian.

FAQs

Hosting

Q: For optional features that require the use of Identity Guardian with Zebra DNA Cloud, in which region is Zebra DNA Cloud hosted and where is the data stored?

A: Zebra DNA Cloud services are accessible worldwide. Currently, the service operates from within the United States, with data stored in the U.S. Zebra is investigating expansion into other regions. For requests regarding regional support, please contact Zebra.

Access Control

Q: Do all users have unique IDs for all systems and applications?

A: Yes

Q: Are generic IDs restricted from performing administrative or privileged functions?

A: Yes

Q: Does your organization enforce a policy to revoke user IDs after a specified time of inactivity?

A: Yes

Q: What is the specified period of inactivity?

A: 3 months

Q: Are complexity requirements (i.e., special characters, numbers, upper case, lower case) enforced for all log-ins?

A: Yes

Q: What is the minimum password length enforced?

A: 12

Q: What is the maximum number of days between required password changes?

A: 90

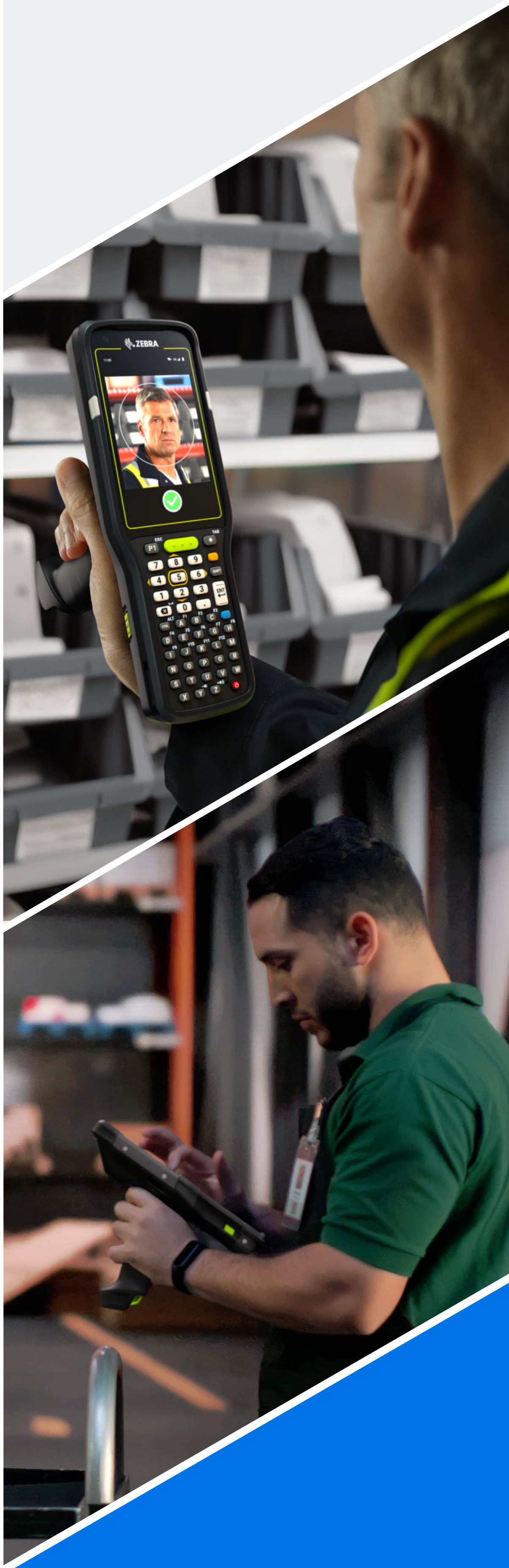
Q: Password Change History—What is the number of password rotations before a previously used password can be re-used?

A: 4

Cryptography

Q: What encryption algorithms are used in IG and what are the key strengths?

A: IG uses a combination of AES-128/256 and RSA-2048



Disaster recovery

Q: What is the current RPO and RTO for the server component?

A: Current RPO is 24 hours and RTO is 24 hours.

Certifications and Compliance

Q: Where can I find information about Zebra Privacy Policies

A: https://www.zebra.com/us/en/about-zebra/company-information/legal/privacy-statement.html

Q: Where can I find information about Zebra Regulatory compliance

A: https://www.zebra.com/us/en/about-zebra/company-information/compliance/declarations-of-conformity.html

Q: Is Identity Guardian ISO 27001 certified?

A: No, IG does not have ISO 27001 Certification

Q: Is Identity Guardian SOC 2 Type 2 certified?

A: No

Q. Identity Guardian requires the device PIN/passcode to be removed. Does this mean that the data on the device is stored in an unencrypted form?

A. On Android devices with File-Based Encryption (FBE) enabled, if the lock screen PIN, password, or pattern is not set, the device still encrypts data using a default password, which is then re-encrypted with the user's credentials if a lock screen is later set

ZEBRA

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com