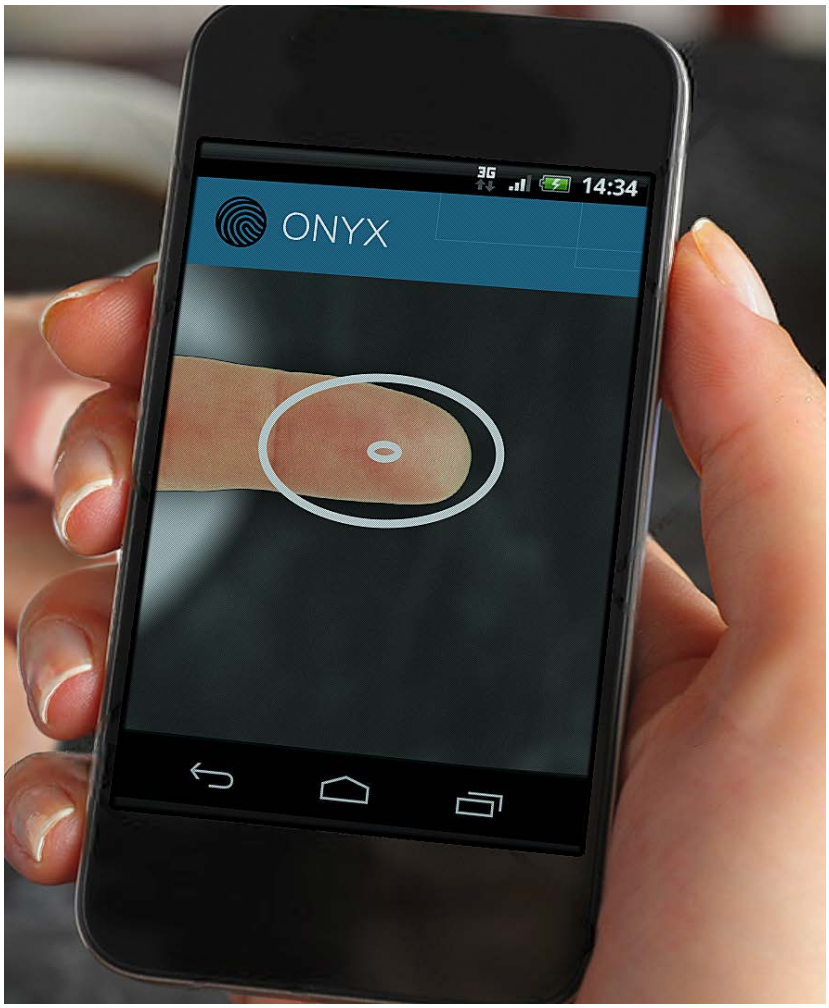
DIAMOND FORTRESS
TECHNOLOGIES

ONYXHD3™

Mobile Touchless Fingerprint Biometrics



Diamond Fortress Technologies | 210 Inverness Pkwy, Birmingham, AL 35242 |
(205) 282-4509 | www.diamondfortress.com

1. Introduction / Background

OnyxHD3™ is biometric "touchless" authentication software developed by Diamond Fortress Technologies. Our product uses a mobile device's camera to capture and identify a user's unique fingerprint. Onyx doesn't require additional hardware, and forever eliminates the need to remember or store passwords and PINs.

Onyx avoids many of the distorting variables present with hardware scanners because it is touchless, resulting in a fingerprint that is a more exact copy of the actual finger. Internal testing and observation has revealed that Onyx creates fingerprints for matching which are superior to those created by hardware scanners. Accordingly, fingerprints generated by Onyx result in more accurate matches. More accurate matches equal greater security. Greater security available to mobile device users right now by only a simple software download, without the need for any additional hardware, resulting in a drastically reduced cost.

2. Business Case: The Future of Mobile Authentication...Today

Usage of biometrics is not anymore a question of “why?”, the questions are now “which one?”, “where?” and “when?” Onyx addresses the following business issues:

- **Data breach and data theft in enterprises:**
    - passwords stolen, transferred
    - smartcards forgotten, lost, stolen, transferred
- **Identity theft**
    - unauthorized prescriptions
    - unauthorized building access
    - unauthorized social welfare services
- **Skimming, Fraud**
    - manipulated ATMs
    - manipulated e-banking
    - manipulated ID cards

A recent report from biometricupdate.com shows that there is a race to incorporate fingerprint biometrics among leading mobile device manufacturers.
Analyst Brian White of Topeka Capital Markets compared Apple's fingerprint scanning technology to Siri, the defining feature of the iPhone 4S when it launched in 2011. He -- and others -- believes a secure fingerprint reader will be continue to be a main selling point of an "iPhone 5S." Because Onyx is a software library, we can be first-to-market with a new class of touchless biometric authentication...one that not only outperforms touch-based sensor solutions, but one that can be offered at a fraction of the cost.

3. ONYX: First-of-its-kind Biometric Security

Our mission is to bring fundamental change in the way businesses and users interact on mobile devices. We give businesses more flexibility in delivering their data, products, and services, while providing their customers with a game-changing combination of increased security and convenience.

a). Technology

Onyx is a software library written in C++, wrapped with Java for use on Android and Objective C for use on iOS, that acquires, processes, and matches images captured with the rear-facing camera of mobile devices.

- Accuracy: the high res images we capture from a mobile devices' camera are "normalized" with our software resulting in more accurate fingerprint rendering and identification.
- Reliability: our touchless solution is more reliable than touch-based or capacitive authentication solutions which are subject to inherent physical limitations, including their vulnerability to wear and tear. Many other solutions have had problems dealing with different age groups and certain ethnicities; however, our internal tests have yielded excellent results in these areas.
- Faster, Broader Deployment: unlike the more common hardware solutions, ours is entirely software-based, which gives us the ability to deploy Onyx on most mobile devices that have a rear-facing camera..
- As manufacturers iterate and improve their camera/lens technology, they are simultaneously improving the accuracy of our authentication.

- Ease-of-Integration: Onyx can be quickly and easily integrated into a broad array of systems. Since it is software, any customization can be done on-the-fly without any form factor redesign.
- Upgradeability: our ability to push out over-air upgrades, fixes, and updates, enables us to continually improve the user experience and "future proof" our technology.

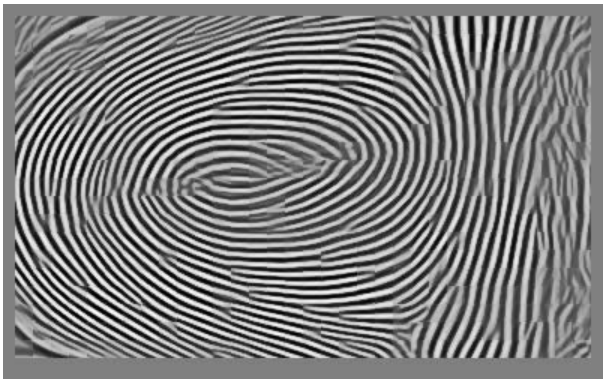
b). How it works

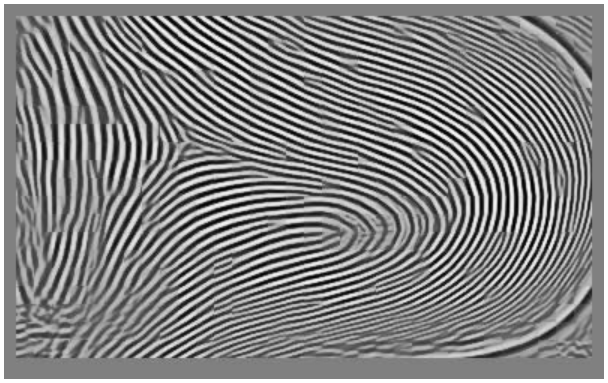
The user places their fingerin view of the rear facing camera. They then center that finger inside the on screen oval.

The user's finger should be approximately 3-4 inches from the back of the phone, as this is the minimum focal distance of most smart phone cameras. Users must make sure their fingertip is approximately the size of the ellipse on the screen.

Once the finger is in place, the finger detection algorithms trigger the autofocus and automatically acquire the finger image.

Images (actual captured fingerprint images)





c). Deployment Models

- **Device-based Solution**: securely stores all user fingerprint information and performs all authentication functions on the mobile device, thereby providing the greatest available control of personal identity information. This solution is perfect for device access authentication, application authentication, and e-commerce authentication. By utilizing the existing cameras available on mobile smart devices, with just an easy software download any individual can experience the benefits of biometric authentication -- without the need to purchase expensive peripheral hardware or a new device with an integrated biometric sensor. Diamond Fortress' Device-Based Solution is a product of our dedication to user identity protection.
- **Server-Based Solution**: enables mobile devices to capture and process fingerprint images for authentication. Once processed on the mobile device the template is securely transported to a remote server for matching against fingerprint images stored on the remote server. Diamond Fortress' Server-Based Solution is ideal for enterprise authentication where users regularly join and leave the system. It can be integrated into limitless applications such as existing physical facility access control systems and enterprise network authentication systems. This enables system administrators to easily control roles, permission sets, and add or remove users, while ensuring the highest degree of confidence that access is being granted only to approved users.

d). Additional Features in Next SDK

- User Experience Improvements
- Improved Scale Tolerance
- Improved Rotation and Angle Tolerance

4. Implementation Scenarios

- Financial Transactions Market – mobile banking; point-of-sale purchases; mobile stock trading; currency transfers.
- In-App Purchases Market – consumers are making more purchases within mobile applications and enhanced security is desired by both businesses and consumers to prevent fraud.
- Mobile Device Management Market – enterprise solutions for identification and verification to protect proprietary, confidential and personal data; handle BYOD management, network infrastructure access.
- Health Care Industry – easy and inexpensive identification of medical care providers, pharmacists, patients, anyone who views or stores medical records or works in a medical facility as required by law; Onyx is also a perfect fit for mobile prescription-writing devices which are becoming more prevalent.
- Border Control / Misc. Govt. Solutions – fills enormous need to protect borders from illegal entry, identification of immigrants and other border security issues, plus innumerable other security uses.
- Login Identification Market – much-needed solution to ensure identity of person accessing a device, an application or the internet.
- OEM Market – we are already working with original equipment manufacturers to provide their clients with custom devices which incorporate touchless biometric security, the possibilities are limitless.
- Physical Facility Access Control – countless organizations are seeking a trustworthy biometric solution to control access to their facilities; we have begun to speak with some and have a tentative deal with a national 24-hour gym; the potential revenue is enormous.
- Law Enforcement – evidence management/chain of custody software is becoming more widespread and our technology would enable providers to set themselves apart from the competition – at least for the short term until the technology is a necessity.

5. Competitor Analysis

At present there are very few mobile phones or devices with built-in biometric hardware. Onyx is the only "touchless" fingerprint solution on the market.

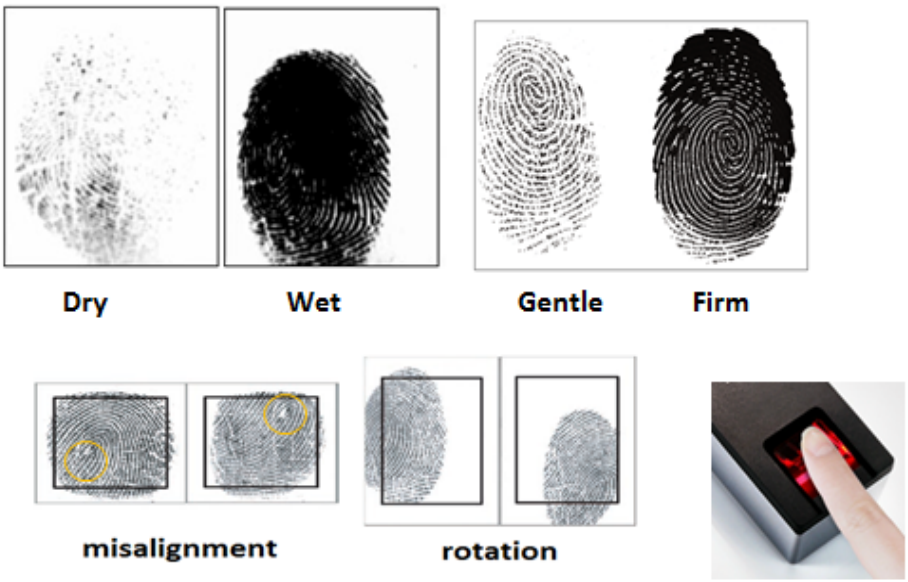
The cost of developing and incorporating such hardware is a significant barrier (as experienced by Apple and Samsung -- see below). Add-on devices were the only widley available option until 2012 saw the introduction of a handful of devices with built-in biometric hardware. Our software-based authentication approach using the device's native hardware (i.e. camera) offers a huge advantage.

	Synaptics (Validity Sensors)	**CrucialTec**	**Apple (AuthenTec)**
Performance (based on FAR/FRR, FER, processing speed)	FAR/FRR performance with as few as one false accept in one million swipes. A nearly 100% enrollment rate. (from company website)	"We're told that the failure rate – or how often it falsely accepts a non-user or fails to recognize your print – is miniscule." (Digitaltrends)	AuthenTec user forum indicates (anecdotal) issues with enrollment of fingerprints for authentication (i.e., "I cannot log on to Windows, keep getting the authentication error. But the fingerprint reader works once I log on manually.")
Implementation	Sensor with customizable ID, a control IC, software for integration into a mobile environment. Buttons provide another method of integrating fingerprint sensors into mobile platforms. A validity sensor was recently packaged and released with the Samsung Galaxy S5.	Biometric scanner built into a home button on a custom case. Fingerprint scanning to lock and unlock phone. The ability to assign a different function to each of your 10 fingers	Via Apple's acquisition of Authentec, the iPhone 5S was released with a fingerprint sensor and system called TouchID; however, Apple does not permit third party use of this sensor

Notes:

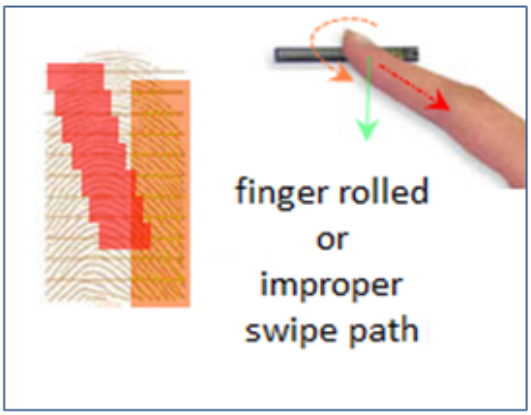
- Highest fingerprint image quality per NIST standards.
- The Failure to Enroll Rate or FER is the percentage of the population which fails to complete enrollment. Such failures can be due to lack of training on how to enroll, to environmental or ergonomic conditions, or to certain demographics which make the biometric modality not suitable for a certain percentage of the population.

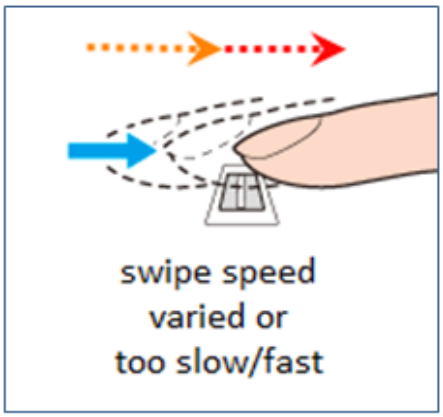
- Most manufacturers of biometric devices do not give clear numbers on the time it takes to enroll as well on the time for an individual to be authenticated or identified using their application.
- Touch-based sensor types experience FRR issues due to environmental conditions or incorrect use. Foreign matter on the fingerprint such as oil and grease, skin dryness, and the age of the person being fingerprinted can result in higher FRR. The finger typically needs to be applied on the sensor in the same manner (same position, same direction) and with uniform pressure (e.g., avoid pressing while twisting). The more finger area the sensor "sees", the better. FRR tends to lower when a user gains more experience on how to use the biometric device or software. Many of these issues are avoided by Onyx due to the touchless modality.
- At close to 100% enrollment rate, Onyx meets or exceeds those by competitors who've published their enrollment rates. Processing time (from enrollment to authentication) is –.7-.9 seconds (per the specs included below).



Touch based sensor systems struggle with various factors which negatively impact image collection and matching.

Touch based sensor systems struggle with various factors which negatively impact image collection and matching.





6. Spec Sheet

- Stored Template File Size: approx. 265 kb
- Image collected at: 1000 – 2000ppi and scaled to 500ppi
- Operating Range: 4 - 6 Inches
- Processing Time: .7-.9 sec
- Enrollment: Yes
- Matching Modes: One to One & One to Many
- Minimum Camera Requirements: 1.5 MP
- Camera Controls: Auto-focus; Manual & Auto-Capture; Manual & Auto-LED control
- OS Compatibilities: iOS, Android, Windows 2000/2003/XP/Vista/7
- Security: Onyx Templates can be encrypted via RSA and AES 256-bit encryption and transferred over network via SSL and TLS encryption protocols.

About Diamond Fortress Technologies

DFT is poised to be an industry leader in the mobile biometrics market, which currently produces annual revenue of $21B. Furthermore, the solutions we offer cross over into numerous markets projected to soon total hundreds of billions of dollars per year. Our technology is second to none; our strategies are sound, and our leadership strong; DFT will provide the safest, fastest and most accurate biometric technology in the market. For more, visit www.diamondfortress.com.