# DeepShield Mobile Security Architecture Guide

**Document Version: 3.2.1**

**Last Updated: January 11, 2024**

**Classification: CONFIDENTIAL - Internal Use Only**

## 1. Introduction

This Security Architecture Guide ("Guide") documents the security architecture, protocols, and implementation requirements for DeepShield Systems, Inc.'s ("DeepShield") mobile security components within the DeepShield Industrial Control System Security Platform ("Platform"). This Guide is a controlled document subject to DeepShield's Information Security Policy.

## 2. Scope and Applicability

1. This Guide applies to all mobile components, applications, and interfaces that interact with DeepShield's Platform, including:

- DeepShield Mobile Command Center (iOS/Android)
- DeepShield Field Operations App
- Mobile API Gateway Services
- Remote Authentication Components
- Mobile Push Notification System

2. All development teams, security architects, and implementation partners must adhere to the architecture standards defined herein.

## 3. Mobile Security Architecture Overview

1. **Core Security Layers**

- Application Layer Security
- Transport Layer Security
- Data Layer Security
- Device-level Security Controls
- Network Communication Security

2. **Authentication Framework**

The mobile security architecture implements multi-factor authentication using:

- Biometric verification (when available)
- Hardware-backed key storage
- Certificate-based authentication
- JSON Web Token (JWT) with RS256 signing

3. **Data Protection**

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Secure key storage using platform-specific keystores
- Zero-knowledge encryption for sensitive OT commands

## 4. Implementation Requirements

1. **Mobile Application Security**

- Mandatory code signing with DeepShield certificates
- Runtime integrity checking
- Anti-tampering controls
- Secure storage of credentials using platform security features
- Prevention of screen capture in sensitive areas

2. **API Security**

- Mutual TLS authentication
- API request signing
- Rate limiting
- Request validation
- Security headers implementation

3. **Secure Communication**

- Certificate pinning
- Custom protocol handlers for OT commands
- Encrypted payload containers
- Secure session management

- Real-time connection monitoring

## 5. Cryptographic Standards

1. **Required Algorithms**

- Symmetric Encryption: AES-256-GCM
- Asymmetric Encryption: RSA-4096
- Hashing: SHA-384
- Key Exchange: ECDHE P-384
- Digital Signatures: Ed25519

2. **Key Management**

- Automatic key rotation every 90 days
- Secure key distribution using DeepShield KMS
- Hardware Security Module integration where available
- Backup key escrow procedures

## 6. Mobile-Specific Security Controls

1. **Device Security Requirements**

- Minimum OS version requirements
- Device integrity verification
- Jailbreak/root detection
- Secure boot verification
- Hardware security capabilities detection

2. **Application Security Controls**

- Automatic session termination after 15 minutes of inactivity
- Secure clipboard handling
- Prevention of runtime debugging
- Application data isolation
- Secure logging practices

## 7. Compliance and Audit

1. **Security Compliance**

- NIST Cybersecurity Framework alignment
- IEC 62443 compliance requirements
- NERC CIP standards adherence
- ISO 27001 controls implementation

2. **Audit Requirements**

- Quarterly security assessments
- Annual penetration testing
- Continuous compliance monitoring
- Security logging and reporting

## 8. Legal Notices and Disclaimers

This document contains confidential and proprietary information of DeepShield Systems, Inc. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of DeepShield Systems, Inc.

The security architecture described herein is subject to continuous improvement and may be updated without notice. Implementation of these security controls must be validated against the most current version of this Guide.

## 9. Document Control

Document Owner: Dr. Elena Rodriguez, Chief Security Architect

Technical Reviewer: James Morrison, VP of Engineering

Legal Reviewer: Corporate Legal Department

Next Review Date: July 11, 2024

---

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024