Technical Proposal for Enhancing NTMC Security with Biometric Login and Multi-Factor Authentication (MFA)

Prepared for:

National Telecommunication Monitoring Centre (NTMC)

Prepared by:

REVE Systems

REVE Centre, Plot-94, Sheikh Hasina Sarani,

Purbachal, Dumni, Khilkhet, Dhaka 1229

www.revesoft.com

Date:

July 1, 2024

Reference No: RSL/NTMC/MFA-V2.0

Confidential

This document contains confidential and proprietary information. Unauthorized use, disclosure, or reproduction is prohibited.

Introduction

In the modern era of cybersecurity threats, ensuring secure access to sensitive data and systems is paramount for any organization, particularly within governmental agencies. The National Telecommunications Monitoring Center (NTMC) plays a crucial role in monitoring and securing telecommunications infrastructure. Given the sensitive nature of its operations, it is imperative that NTMC enhances its security measures to protect against unauthorized access and potential breaches.

This technical proposal outlines a comprehensive strategy for enhancing NTMC's security through the implementation of biometric login and multi-factor authentication (MFA). The proposed solution aims to fortify access control by integrating advanced biometric authentication methods, including fingerprint and face recognition, coupled with traditional password-based security.

The proposed implementation will be conducted in two phases.

Phase 1: Fingerprint Authentication
Module 1: Extend Keycloak SPI with Fingerprint Authentication
Module 2: AD Authentication with Fingerprint

Phase 2: Face Authentication
Module 3: Extend Keycloak SPI with Face Authentication
Module 4: AD Authentication with Face

Purpose

To ensure secure access for designated users to desktops and applications using biometric and multi-factor authentication (MFA).

Objectives

1. **MFA Solution Implementation:**
   - Deploy a comprehensive MFA solution across all desktops and applications within the government agency.
2. **Local User Authentication:**
   - Authenticate local users through various Active Directory environments using MFA for enhanced security.
3. **Remote User Authentication:**
   - Enable secure access for remote users to web applications via MFA, ensuring data integrity and user verification.
4. **Biometric and Password Authentication:**
   - Utilize biometric methods (fingerprint/face recognition) combined with passwords to ensure unique and robust user verification.
5. **Support for Internet and Non-Internet Zones:**

- Provide authentication solutions suitable for both internet-connected and non-internet environments, ensuring seamless access control.

Detailed Technical Specifications:

1. General

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
1.1	User Accessibility	Establish a comprehensive system for user accessibility to workstations with biometric and MFA.	Yes	Ensures secure access to application via biometric authentication and MFA, enhancing user security and compliance with organizational policies.
1.2	Active Directory Association	Associate with multiple Active Directories:	Need to explore	Supports integration with ORGANIZATION ADDC (no internet), ADDC (internet), and remote users (internet) using secure LDAP and federation services like ADFS, ensuring seamless authentication across different environments.
		i. ORGANIZATION ADDC (no internet)		
		ii. ORGANIZATION ADDC (internet)		
		iii. ORGANIZATION remote user (internet)		
1.3	Authentication Methods	Authenticate with username, password, and biometric matching.	Yes	Combines traditional credentials with biometric (fingerprint/face) verification, meeting NIST SP 800-63B guidelines for enhanced security and user verification.
1.4	Biological Authentication	Serve biological authentication by collecting 4-4-2 fingerprint data and 3D face recognition.	Need to explore	Implements advanced biometric data collection for accurate user identification and authentication, enhancing security measures.

1.5	Scalability	Solution should be scalable to accommodate changing user numbers. Present scope: 1000 user licenses with 1000 fingerprint and 3D face image scanner.	Yes	Scalable architecture supports growth and expansion without compromising performance or security standards.
1.6	User Information Updates	Solution should be able to update user information.	Yes	Ensures timely updates to user profiles and credentials, maintaining accuracy and compliance with organizational policies.
1.7	Application Updates	Solution should be able to update and upgrade applications free of cost to mitigate dependencies on Active Directory, operating system, or Keycloak versions.	Yes	Ensures seamless updates and upgrades to maintain compatibility and security, minimizing operational disruptions.
1.8	Licensing Model	The entire solution licensing model must be perpetual.	Yes	Ensures ongoing support and updates with a perpetual licensing model, providing cost predictability and long-term value.
1.9	Fingerprint Data Validation	Validate user fingerprint data with a 1:1 relationship to the NID database.	All kinds of NID verification part Skipped. Confirmed from NTMC.	Ensures accuracy and reliability of biometric data verification, enhancing overall system security and user trust. Need to explore fingerprint data store procedure into NID side.

2. User Management System

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
2.1	User Roles	System should have user roles: Super administrator, Admin, Auditor User.	Yes	Differentiates user privileges based on roles, ensuring secure access

				control and operational integrity.
2.2	Super Administrator	Super admin will administer the entire system.	Yes	Manages system-wide configurations, ensuring governance and compliance with organizational policies.
2.3	Admin Responsibilities	Admin responsibilities include enrollment, re-enrollment, and removal of users; testing, verification, validation, and approval of the system.	Yes	Ensures efficient management of biometric system operations, maintaining data accuracy and system integrity.
2.4	Auditor Responsibilities	Auditor user responsibilities include reviewing access, activity, change logs, denial of access, and system downtime logs.	Yes	Monitors and audits system activities, ensuring compliance with security policies and regulatory requirements.

3. System Architecture

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
3.1	System Architecture Design	Propose system architecture design with a data flow diagram.	Yes	Illustrates the flow of authentication requests and data exchange within the system architecture, ensuring clarity and alignment with organizational requirements.
3.2	MFA System Architecture	Propose multi-factor authentication system architecture, including port mapping onto hardware and software components.	Yes	Integrates MFA components with existing infrastructure, optimizing performance and security of authentication processes.

4. Operations

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
4.1	Biometric Policy Alignment	Propose the biometric policy aligned with the security policy of the organization.	Yes	Ensures that biometric authentication methods comply with organizational security policies, addressing confidentiality, integrity, and availability (CIA) of biometric data.
4.2	CIA of Biometric Information	Propose security measures to maintain confidentiality, integrity, and availability (CIA) of biometric information.	Yes	Implements safeguards to protect biometric data from unauthorized access, tampering, or loss, ensuring its availability for authentication purposes.
4.3	System Monitoring	Propose monitoring of biometric system efficiency through data analysis (e.g., enrollment time, success/failure rates).	Yes	Monitors system performance metrics to evaluate efficiency and reliability of biometric authentication processes, optimizing system uptime and user experience.
4.4	Data Storage Requirements	Define data storage capacity requirements for biometric data.	Yes	Determines storage needs to accommodate biometric templates (fingerprint, 3D face scans) securely and efficiently, ensuring scalability and compliance.
4.5	Backup and Restore Procedures	Outline procedures for regular data backup and restore operations.	Yes	Establishes protocols for data backup to prevent loss of biometric templates and system configurations, enabling quick recovery in case of data loss or corruption.
4.6	Upgrade and Patch Management	Define procedures for managing system upgrades and patches.	Yes	Ensures timely deployment of updates to address security vulnerabilities and enhance system functionality, minimizing risks associated with outdated software.
4.7	Business Continuity	Outline strategies for business continuity in case of biometric system failure.	Yes	Implements contingency plans and standby systems to maintain continuous service availability, ensuring

				uninterrupted user access and operational continuity.
4.8	Change Control	Implement appropriate change control processes where role-based access is used.	Yes	Ensures controlled implementation of changes to biometric system configurations or policies, mitigating risks of unauthorized modifications or disruptions.

5. Dashboard

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
5.1	Separate Dashboards	Implement separate dashboards for different scenarios (as per section 1.2).	Yes	Provides dedicated dashboards tailored to monitor and manage user access and authentication activities across various Active Directory environments and remote users.
5.2	Real-Time Monitoring	Provide real-time information on failed login attempts, security events, and device statuses (e.g., compromised devices).	Yes	Enables immediate detection and response to security incidents and anomalies, enhancing overall system security posture and user protection.

6. Security Privileges

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
6.1	Real-Time Information	Provide real-time information on security-related events (e.g., failed login attempts).	Yes	Offers instant visibility into security incidents and threats, facilitating prompt action and mitigation to safeguard system integrity and user data.
6.2	Alarm System	Implement different color codes for designated alarms (e.g., security breaches).	Yes	Enhances incident response capabilities by categorizing alarms based on severity or type, ensuring prioritized and efficient security incident management.

7. Necessary Hardware and Software

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
7.1	Hardware Requirements	Propose detailed list of necessary hardware for deploying 1000 fingerprint and 3D face image scanners, along with required software.	Yes	Specifies hardware components (scanners) and software infrastructure needed to support biometric authentication across the organization, ensuring scalability and performance. **List of Proposed sample Fingerprint Scanners** **1. Suprema** • **Model**: RealScan-G10 • **Description**: High-quality optical fingerprint scanner known for accuracy and reliability in large-scale deployments. **2. HID Global (formerly Crossmatch)** • **Model**: Guardian 200 • **Description**: Robust fingerprint scanner with durable construction and high-resolution imaging capabilities. **3. Integrated Biometrics** • **Model**: Columbo • **Description**: Lightweight and mobile FBI PIV FAP 30 certified fingerprint scanner suitable for various environments. **4. Idemia (formerly Morpho)**

				- **Model**: MorphoWave Compact - **Description**: Touchless fingerprint scanner using 3D imaging technology for fast and hygienic authentication. **Aratek** - **Model**: Ten-Print FBI FAP 60 4-4-2 Live-Scan Fingerprint Scanner (A900) - **Description**: High-performance ten-print live-scan fingerprint scanner compliant with FBI FAP 60 standards, suitable for high-security applications. **List of Proposed sample 3D Face Image Scanners** **1. Intel RealSense** - **Model**: D415 - **Description**: Compact 3D camera with depth sensing for capturing detailed facial data, suitable for biometric applications. **2. Microsoft** - **Model**: Azure Kinect DK - **Description**: Advanced 3D camera system with high-fidelity depth sensing and RGB camera, ideal for accurate facial recognition. **3. Cognitec Systems**

				- **Model**: FaceVACS-3D - **Description**: Specialized 3D face recognition technology offering high accuracy and reliability in biometric identification.
7.2	Supported Scanners	Provide a list of fingerprint scanners compatible with the proposed solution.	Yes	Identifies specific models of fingerprint scanners capable of integrating seamlessly with the biometric authentication system, meeting technical and operational requirements. Sample list given at 7.1
7.3	Sizing and Storage Calculations	Calculate sizing and storage requirements to support the proposed system, ensuring scalability, redundancy, and fault tolerance.	Yes	Determines storage capacity and processing power necessary to handle biometric data securely and efficiently, accommodating future growth and operational demands.
7.4	Hardware Architecture	Ensure hardware architecture is independent and flexible for scalable deployment as required by the organization.	Yes	Designs scalable hardware infrastructure capable of expanding to meet increased user demands and organizational growth, optimizing system performance and usability.
7.5	Warranty and Support	Ensure hardware and software service support warranty for 3 years.	Yes	Provides assurance of support and maintenance for hardware and software components over a defined period, minimizing operational risks and disruptions.
7.6	Operational Elements	Ensure all necessary elements related to hardware to keep the system operational and functional.	Yes	Ensures availability of essential hardware components and peripherals required for ongoing system functionality and user access.
7.7	OS Compatibility	Ensure proposed MFA solution supports existing operating systems.	Yes	Confirms compatibility with current organizational operating systems, ensuring seamless integration and functionality.

8. Log Management

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
8.1	MFA Activities Logs	Maintain logs of MFA activities conducted by users, containing comprehensive information related to activities and users.	Yes	Records detailed logs of user authentication and system access activities, facilitating auditing and compliance with security policies.
8.2	Access Control	Restrict access to audit trail logs and alarms to authorized personnel only.	Yes	Ensures confidentiality and integrity of audit trail data, limiting access to authorized personnel for security and compliance purposes.
8.3	Data Security	Ensure all data in logs are read-only by default to prevent unauthorized alterations.	Yes	Prevents unauthorized modifications to audit trail data, maintaining data integrity and reliability for auditing and compliance purposes.
8.4	Data Retention	Implement no-deletion policy for events logged in the system.	Yes	Preserves all logged events without deletion, ensuring comprehensive audit trail for forensic analysis and compliance audits.
8.5	Log Reporting	Provide filter options to generate required log reports as per organizational needs.	Yes	Facilitates customized reporting of audit trail data based on specific criteria, enabling timely and accurate analysis for security and compliance purposes.

9. Report Generation

Ser.	Scope	Detail Technical Specification	Remarks	Description of Remarks
9.1	Report Formats	Provision for report generation using intuitive timeline view,	Yes	Offers multiple formats (PDF, CSV, XLS, etc.) for generating comprehensive reports,

		grid view, graphs, charts, profiles, etc.		enhancing data visualization and analysis capabilities.
9.2	Export Options	Export reports in different formats (PDF, CSV, XLS, etc.).	Yes	Facilitates easy export of generated reports into various formats, supporting flexible data sharing and presentation for different stakeholders.
9.3	Department-wise Statistics	Provide detailed statistics reports for users categorized by departments.	Yes	Delivers department-specific insights and metrics, enabling targeted analysis and monitoring of user activities and system performance.

MFA Implementation Phases:

Phase 1: Fingerprint Authentication

Module 1: Extend Keycloak SPI with Fingerprint Authentication

Description:
Integrate fingerprint authentication into the existing Keycloak authentication flow by extending the Service Provider Interface (SPI).

Approach:

- Analyze the current Keycloak setup and authentication flow.
- Develop a custom SPI extension to incorporate fingerprint authentication.
- Implement a user interface for capturing and verifying fingerprints.
- Test the integration to ensure it meets security and performance standards.

Deliverables:

- Custom SPI extension for fingerprint authentication.
- Documentation and user guide for the new authentication method.

Module 2: AD Authentication with Fingerprint

Description:
Enable fingerprint-based authentication for Active Directory (AD) users.

Approach:

- Analyze the existing AD authentication mechanisms.
- Develop and deploy a solution to integrate fingerprint authentication with AD.

- Ensure compatibility with existing AD policies and user management tools.
- Test the solution to confirm it meets NTMC's security requirements.

Deliverables:

- AD integration with fingerprint authentication.
- Comprehensive documentation and user manual.

Phase 2: Face Authentication

Module 3: Extend Keycloak SPI with Face Authentication

Description

Implement facial recognition as an additional authentication method within the Keycloak authentication flow.

Approach

- Analyze the current Keycloak setup and authentication flow to accommodate facial recognition.
- Develop facial recognition algorithms using deep learning models, such as Convolutional Neural Networks (CNNs).
- Extend the Keycloak Service Provider Interface (SPI) to integrate facial biometrics.
- Implement liveness detection techniques to prevent spoofing attacks.
- Conduct rigorous testing to ensure accuracy and reliability under various conditions.

Deliverables

- Custom SPI extension for face authentication in Keycloak.
- User interface components for facial registration and authentication.
- Documentation and user guide detailing setup, configuration, and usage instructions.

Module 4: AD Authentication with Face

Description

Integrate facial recognition authentication with Active Directory (AD) for NTMC users.

Approach

- Evaluate existing AD authentication mechanisms and policies.
- Develop and deploy a solution to enable facial recognition authentication within the AD framework.

- Ensure seamless integration with NTMC's AD infrastructure and user management tools.
- Implement secure data transmission protocols to protect sensitive biometric information.
- Conduct extensive testing to validate security and compatibility requirements.

Deliverables

- AD integration module supporting facial authentication.
- Configuration guides and integration documentation.
- Training materials for administrators and end-users on using facial recognition with AD.

Conclusion

This phased approach to implementing the MFA solution using Keycloak SPI ensures NTMC enhances its security posture while maintaining usability and scalability. Each phase builds upon the previous one, incorporating additional authentication factors and integrating seamlessly with existing systems. The outlined technical details and workflows provide a clear path for implementation, testing, and deployment, ensuring a robust and reliable MFA solution across NTMC's environment.