Final Security Mechanisms Report

Mobile Plataform	Web Application
Application domain type	m-Health
Authentication	Yes
Authentication schemes	Biometric-based authentication ; Channel-based authentication ; Factors-based authentication
Has DB	Yes
Type of data storage	Local Storage (Centralized Database)
Which DB	
Type of data stored	Confidential Data ; Critical Data
User Registration	Yes
Type of Registration	The users will register themselves
Programming Languages	Java ; HTML5
Input Forms	Yes
Upload Files	Yes
The system has logs	Yes
The system has regular updates	Yes
The system has third-party	Yes
System Cloud Environments	Public Cloud
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	3G ; 4G/LTE ; 5G ; Bluetooth ; Wi-Fi ; GPS ; NFC
Data Center Phisical Access	Yes

In order to guarantee the confidentiality, availability and privacy of shared data and data freshness, at rest, in use or in transit by legitimate users and communications, as well as the integrity and authenticity of data and communications, developers are recommended of apps for the cloud & mobile platform incorporate *secure backup mechanisms* in the implementation and codification phase of the software development process, as described below.

Req	Mechanism	Mechanism Type	Description	Layer
Integrity, authenticity and privacy, authorization, availability, data freshness	Backup	Local and remote encrypted storage using modern and secure encryption schemes	To incorporate remote authentication mechanisms, that is, access to stored data should only be possible through remote authentication	Data Link

				Using NIDS, NIPS, HIDS, HIPS			Allow to guarantee the Network defense in depth
				To incorporate hybrid authentication mechanisms for accessing applications from the mobile device (e.g., fingerprint and PIN, face recognition and PIN or voice and PIN recognition, iris recognition and PIN or PIN)			Application
				To incorporate access control mechanisms that ensure application data isolation and user session management			Application
				Installing IPS and IDS on mobile devices, in order to guarantee the perimeter security of user data stored locally			Network

In order to guarantee the integrity and availability of user data stored in the cloud and consequently their leakage or loss, it is recommended that developers of mobile applications incorporate *audit mechanisms*, based on the illustration below.

Ref	Mechanism	Mechanism Type	Description	Layer
	Confidentiality, Integrity, availability, auditing, accountability	Reliability, inspection, Identity-based public cloud auditing scheme, analysis mechanisms		Data Link

	An identity-based distributed probable data ownership scheme
	Audit scheme for public cloud storage based on authorized identity with hierarchical structure for large-scale user groups

In order to guarantee the confidentiality and privacy of data shared, at rest or in transit by legitimate users and communications, as well as the integrity, authenticity of data and communications, it is recommended to developers of apps for the cloud & mobile platform to incorporate the algorithms cryptographic and related mechanisms in the implementation and codification phase of the software development process, as described below.

Ref	Mechanism	Mechanism Type	Description	Layer
	Privacy and confidentiality authentication	Cryptographic algorithms Confidentiality, related authorization mechanisms	TCP/TLS, HTTPS, XMPP, AES256-RSA, SSL/TLS, HTTPSCurve25519, AES-256, AES256-RSA2048	Encrypted communications Presentation and Application
		MAC, Digital Signatures	Authentication and Application	Presentation and Application
		AES-GCM-256 or ChaCha20-Poly1305	Confidentiality and Application Algorithms	Presentation and Application
		RSA (3072 bits and higher), ECDSA with NIST P-384	Digital Signature Algorithms	Presentation and Application
	Integrity	SHA-256, SHA-384, SHA-512, Blake2		Presentation and Application
		RSA (3072 bits and higher), DH (3072 bits or higher), ECDH with NIST P-384	Key establishment algorithms	Presentation and Application

In order to ensure that personal data, applications and servers are authentic and that they are only accessed by legitimate or authorized entities, it is recommended to incorporate the authentication and backup mechanisms in the implementation and codification phase of the software development process, as described in the table below.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer
Authenticity	Both	Authentication	Biometric-based authentication	Gaze Gesture, Electrocardiogram, Voice recognition, Signature recognition, Gait recognition, Behavior profiling, Fingerprint, Smart card, Multi-touch interfaces, Graphical password, Face recognition, Iris recognition, Rhythm, Capacitive touch-screen, Ear Shape, Arm Gesture, Keystroke Dinamics, Touch dinamics	Application

In order to ensure that personal data, applications and servers are authentic and that they are only accessed by legitimate or authorized entities, it is recommended to incorporate the authentication and backup mechanisms in the implementation and codification phase of the software development process, as described in the table below.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer

Authenticity	Both	Authentication	Channel-based authentication	Physical proximity, Electronic voting, Seamless roaming, Transitive authentication, Atribute-based authentication, User-habit-oriented authentication, Handover authentication	Application
	Both	Secure Boot	Digital Signature, checksums, Trusted Plataform Module	Boot verification of hardware, software and firmware integrity	Application

In order to ensure that personal data, applications and servers are authentic and that they are only accessed by legitimate or authorized entities, it is recommended to incorporate the authentication and backup mechanisms in the implementation and codification phase of the software development process, as described in the table below.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer
Authenticity	Both	Authentication	Factors-based authentication	Two-factor, Three-factor, Multi-factor	Application
	Both	Secure Boot	Digital Signature or checksums	Boot verification of hardware, software and firmware integrity	Application

In order to ensure that the data shared and exchanged between two or more authorized entities are reliable, complete, authentic and only accessible to these entities, it is recommended that software developers for the mobile ecosystem incorporate *cryptographic protocols* in the implementation and codification phase of the software development process, as described below.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer

	Both	Cryptographic Protocols over SCTP/UDP	SSL/TLS, DTLS	Protocols that can be used or implemented over a network to ensure secure data transmission over UDP and SCTP	Application, Presentation, Session
	Both	Wireless Cryptographic Protocols	WEP, WPA, 802.11i (WPA2), EAP, PSK, TKIP, PEAP, EAP-TTLS, EAP-PSK, EAP-SIM, EAP-AKA, AES-CCMP	Security Protocols that must be used or implemented specifically according to the mobile platform or operating system for wireless networks	Transport
	Both	Cryptographic Protocols over IP Protocol	IPSec, PEAP, EAP-TLS	Protocols that ensure data packet encryption and authentication over the IP Protocol	Network and Data Link

In order to ensure that applications and users access only and only the resources allowed, safeguarding the principle of minimum privileges, it is recommended that developers of apps for the cloud & mobile ecosystem incorporate *access control mechanisms* in the coding implementation phase in the software development process, according to the suggestions described below.

Require	Plataform	Mechar	Mechanism Type	Desc	Layer
	Both	Authorization, audit, authenticity, interoperability	Access Control	RBAC, ABAC, ABE	Applic
	Android		DR BACA, CA-ARBAC, RBACA		

To ensure a permanent or almost permanent observation of the system, in order to detect any unexpected activity or detect abuses by privileged users, app developers for the cloud & mobile ecosystem are recommended to incorporate inspection mechanisms in the implementation and coding phase in the software development process, as described below.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer
Privacy, authorization, immunity, Tampering Detection		Inspection	IDS, IPS, NIDS, NIPS, HIDS, HIPS, IDPS, DIDS, VMM based IDS		Network

In order to ensure non-repudiation, audit and accountability by all legitimate or illegitimate entities in the cloud & mobile ecosystem, it is recommended that mobile app developers incorporate *logging mechanisms* during the implementation and coding in the software development process, as described below.

Requirement	Mechanism	Mechanism Type	Description	Layer
Non repudiation, audit, accountability	System, Boot, Logging, System log files or event log		It is recommended that developers during the coding phase, use the native APIs of each Data Link of the mobile device platform that allow incorporation of Logging into application during the software development process	

			All mechanisms related to storage or secure backup apply		

In order to ensure that the application and confidential data of legitimate users are not accessed by third parties from the device or remotely from the data center, it is recommended that users incorporate *tampering detention mechanisms* on the device, as illustrated below.

Requirement	Mechanism	Mechanism Type	Description	Layer
Authorization, authenticity, privacy, immunity	Device authentication, Application authentication, Detection	Incorporation of hybrid authentication schemes to the application		Application
		Incorporation of access control and session management mechanisms that guarantee the sending of notifications whenever there is new access from a new device or browser		Session

In order to ensure that user data stored in remote databases is safe and reliable, app developers for the cloud & mobile ecosystem are recommended to incorporate data *location physical mechanisms* for data centers.

Requirement	Plataform	Mechanism	Mechanism Type	Description	Layer
Physical security	Both	Physical security location	Smartcards, mobile surveillance cameras with 360 degree night vision, motion sensors and detectors, facial recognition identification cameras, etc.		Physical

In order to ensure that applications are resilient to an eventual attack and that they do not violate the principle of minimum requirements when sharing resources locally or remotely, app developers for the cloud & mobile ecosystem are recommended to incorporate *confinement mechanisms*, as well as those of access

control or secure permissions.

Requirement	Plataform	Mechanism	Mechanism Type	Desc	Layer
Privacy, integrity, authenticity, immunity	Both	Containerizing	Sandboxing, TPM, MTM, TEE		Its purpose is to guarant the privacy, integrity and authent of the applic data of the end users and the integrity of the system
	Both		Firewall		
	Both		DMZ		
	iOS		Unix Permissions		
	iOS		iOS Capabilities		
	iOS		Hard-Coded Checks		

In order to ensure that legitimate or illegitimate users or machines do not access users' confidential data or potentially unsafe resources or harmful content to sensitive users or children, app developers for the cloud & mobile ecosystem are recommended to incorporate filtering mechanisms , such as those listed below.

Requirement	Plataform	Mechanism	Mechanism Ty	Description	Layer

Integrity, authenticity, access Control, Privacy	Both	Filtering	Firewall and Cryptographic Techniques		Network