Jellyfish MOBILE

SIM3

Technical Whitepaper

Model Chipset	ST33 Consumer
Package	MFF2 5*6 2.5*2.7
Version	1.2.1
Date	18 Jan 2024

Jellyfish MOBILE

Version	Date	Author	Comments
V1.0	Nov 2023	Ethan	**Initial version**
V1.1	Dec 2023	Ethan	**Added Use Case**
V1.2	Jan 2024	Ethan	**Added Finalized HW Specifications**
V1.2.1	Jan 2024	Ethan	**Updated Cryptography capabilities**

Jellyfish MOBILE

Content

Introduction

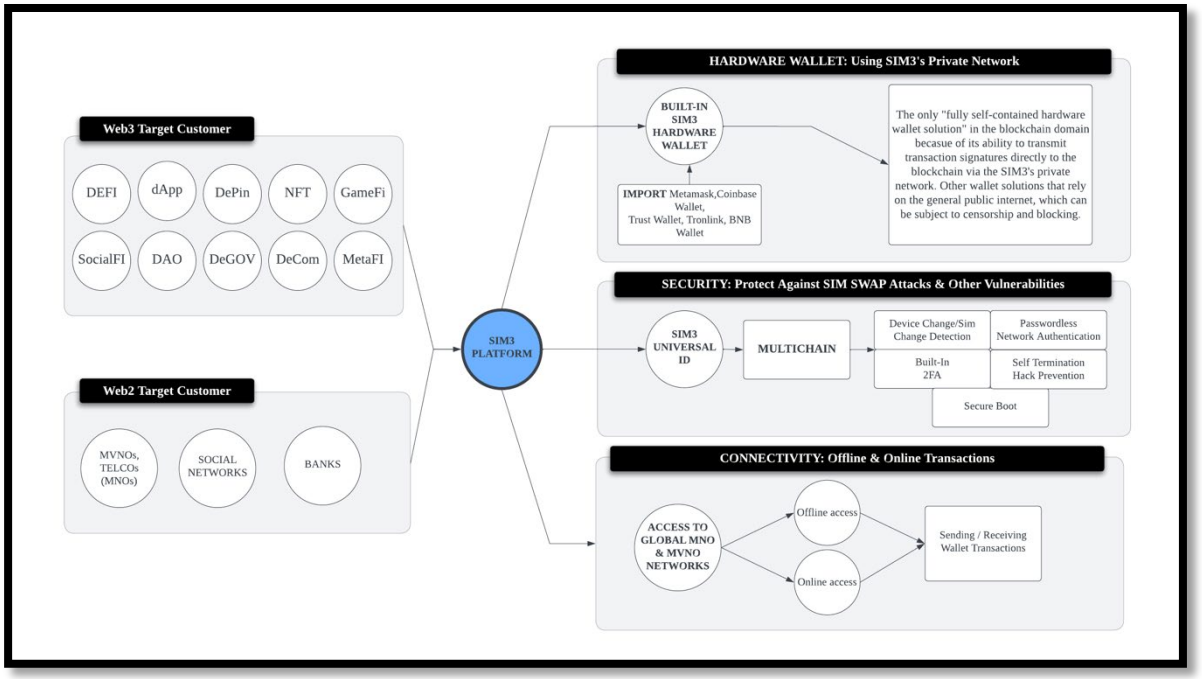
In the rapidly evolving digital landscape, the fusion of mobile telecommunications with blockchain technology presents a transformative opportunity. SIM3 by Jellyfish Mobile stands at this technological crossroads, offering an innovative solution that integrates the security and decentralization of Web3 with the ubiquity and accessibility of mobile technology. This whitepaper delves into the technical nuances of SIM3, a cutting-edge product that redefines the standards of mobile communication and digital asset management.

Technology Overview

SIM3 Architecture

SIM3 is a revolutionary mobile SIM card, architecturally designed to encompass both standard telecommunication functionalities and advanced Web3 capabilities. At its core, SIM3 features a state-of-the-art chipset, compatible with existing mobile devices while integrating a hardware-based Web3 wallet. This wallet facilitates secure, on-the-go management of digital assets, including cryptocurrencies and tokens, directly from the user's mobile device.

The software layer of SIM3 is engineered for seamless interaction with blockchain networks, allowing users to access decentralized applications (dApps) without the need for additional hardware. This integration ensures that users can engage in a wide range of blockchain-based activities, such as token swaps, smart contract interactions, and decentralized finance (DeFi) operations, directly through their mobile phones.



Hardware Wallet Integration

The SIM3 platform is at the vanguard of mobile hardware wallet technology, incorporating a state-of-the-art, ultra-secure hardware wallet directly within the SIM card. This fusion of mobile telephony with blockchain-enabled secure storage propels digital asset management into a new realm of security and operational ease, ideal for the demands of modern mobile users.

Key Features:

- Embedded Security: The SIM3's secure enclave is the bastion that houses the hardware wallet. This secure enclave provides a robust layer of defence against both physical and logical attacks, ensuring that the wallet's integrity remains unassailable.

- Private Key Isolation: At the heart of SIM3's security model is the isolation of private keys. Generated and stored within the secure enclave, these keys are impervious to extraction or compromise by external applications or the device's operating system, ensuring the user's digital assets remain under their exclusive control.

- Transaction Signing: The SIM3 module empowers users to sign transactions with confidence. Leveraging robust encryption algorithms, the SIM3 ensures that every transaction is both secure and indisputable, providing users with the peace of mind that their transactions will be executed as intended.

- Multi-Cryptocurrency Support: Reflecting the diverse landscape of digital assets, the SIM3 hardware wallet is designed for versatility, supporting an array of cryptocurrencies. This capability allows users to manage a broad portfolio of digital assets effortlessly and securely from their mobile device.

Security

Security is a paramount concern in the design of SIM3. The product incorporates several robust security measures:

- Enhanced Encryption: Utilizing advanced encryption standards, SIM3 ensures that all data, both stored and in transit, is protected against unauthorized access and cyber threats.
- Cold Wallet Isolation: The in-built cold wallet is isolated from the phone's operating system, providing an added layer of security for users' digital assets. This isolation shields the wallet from online vulnerabilities, effectively minimizing the risk of hacking and unauthorized access.
- Secure Boot Process: SIM3's boot process is fortified with stringent security checks to prevent tampering and unauthorized modifications of the firmware, ensuring that only trusted software is executed on the device.
- Anti-SIM Swap Technology: Addressing the prevalent threat of SIM swap attacks, SIM3 incorporates innovative features that detect and prevent unauthorized SIM exchanges, safeguarding users' digital identities and assets.

Connectivity

The SIM3 module is equipped with a proprietary private network that enables offline access to blockchain networks. This innovative feature ensures that users can perform critical blockchain operations even in the absence of traditional internet connectivity.

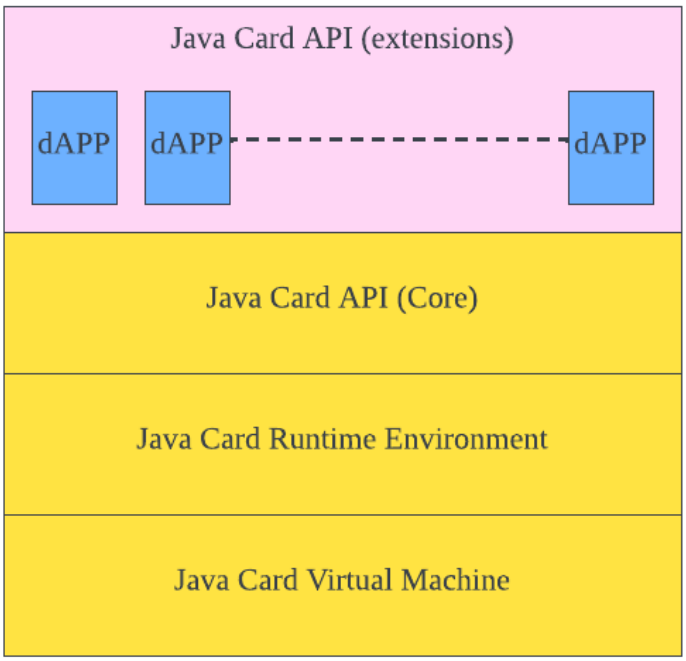
Online/Offline Access Capabilities:

- Decentralized Application (dApp) Interaction: Users can interact with dApps and execute smart contracts while offline, with transactions queued for broadcast once connectivity is restored.
- Seamless Swaps and Transfers: The SIM3 enables offline initiation of token swaps and transfers, providing convenience and continuity in managing digital assets.
- Resilience to Network Outages: By allowing blockchain interaction through the SIM3 private network, users are safeguarded against disruptions due to network outages or cyber attacks targeting online infrastructure.

SIM3 Application Details

SIM3 Architecture: Java Card Platform

The architecture of the SIM3 is anchored in the Java Card Virtual Machine (JCVM), which provides a secure and interoperable execution environment for Java Card applets. The JCVM is essential for the execution of bytecode, translating high-level instructions into actions within the SIM3's secure element. The SIM3's architecture is designed to prioritize security, interoperability, and resource efficiency, catering to the diverse needs of Java Card application development within the secure confines of a SIM card environment.



SIM3 Platform

Java Card Virtual Machine (JCVM)

- The JCVM serves as the execution engine for Java Card applets, providing a robust environment that supports Java's object-oriented paradigm within the resource-constrained context of a SIM card. It manages the low-level interactions with the hardware, abstracting the complexity of the secure element for applet developers.

Java Card Runtime Environment (JCRE)

- Directly interfacing with the JCVM is the JCRE, which is responsible for managing the applet lifecycle, enforcing security policies, and facilitating object sharing among applets in a multi-application setting. It provides the necessary runtime libraries and APIs that applets rely on during execution.

Java Card API (Core)

- The core Java Card API layer offers a comprehensive suite of services crucial for the development of secure and interoperable applets. This includes cryptographic services, personalization capabilities, and secure communication protocols. The core API acts as a mediator between the applets and the JCRE, translating high-level requests into secure operations.

Java Card API (Extensions)

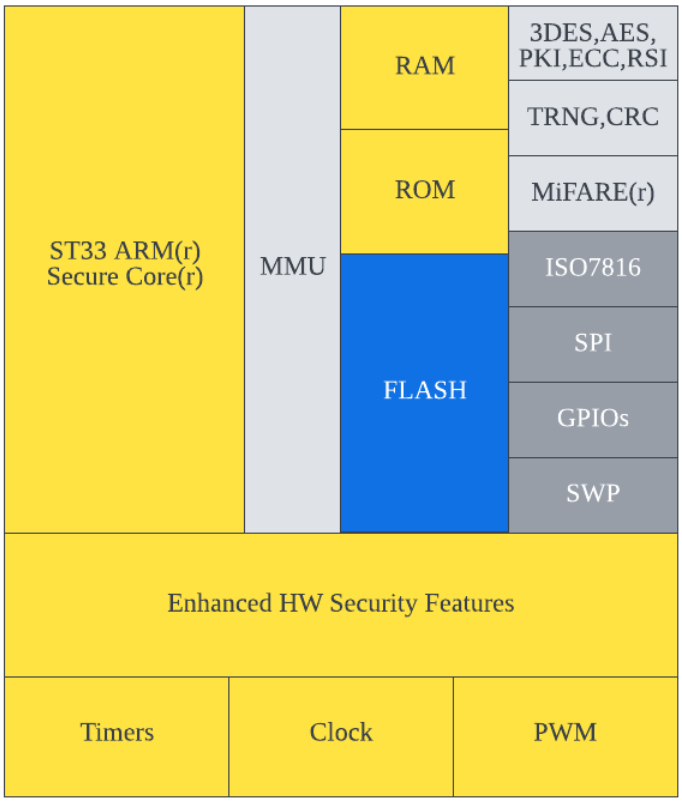
- Atop the core API, the extensions layer allows for the development of custom applets with specialized functionalities. This layer represents the extensibility of the Java Card platform, enabling developers to innovate beyond the standard API offerings.

Configurability

- The architecture supports dynamic configuration parameters, allowing optimization of the JCVM, JCRE, and Java Card API layers according to the specific resource constraints of the hardware platform. This includes settings for heap and stack sizes, transient memory, and transaction buffer sizes, ensuring the platform remains flexible and adaptable to various deployment scenarios.

Cryptographic Implementation for the SIM3 Platform

The SIM3 hardware wallet, powered by the ST33 chip, employs a range of advanced cryptographic algorithms, each suited for specific blockchain protocols. This tailored approach ensures optimal security and performance for various digital currencies.



ST33 ARM Core

ECC for Bitcoin and Ethereum

- Elliptic Curve Cryptography (ECC): The ECC co-processor within the ST33 chip is pivotal in generating and securely managing wallet keys, which are the cornerstone of user interaction with blockchain networks. ECC is a preferred cryptographic method for its balance of security and computational efficiency.
- Bitcoin: Bitcoin utilizes the secp256k1 elliptic curve for its cryptographic operations. This particular curve was chosen for several reasons, including its efficiency in computation and its large prime order, which enhances security. When a user generates a Bitcoin wallet, the ECC co-processor creates a private key, which is a randomly selected number from the finite field defined by secp256k1. The corresponding public key is then computed as a point on the elliptic curve by multiplying the private key with the curve's base point, G. The public key can then be hashed and encoded to produce a Bitcoin address.
- Ethereum: Ethereum also leverages elliptic curve cryptography for wallet key generation, employing the same secp256k1 curve as Bitcoin. Ethereum's use of this curve allows for the creation of a unique public-private key pair that forms the basis of an Ethereum address. The process mirrors Bitcoin's key generation, ensuring that the integrity and security principles provided by the secp256k1 curve are maintained.

Other Layer 1 (L1) Chains:

- L1 chains such as Litecoin, Ripple, Dash, and others, may use secp256k1 or different ECC curves like secp256r1 or ed25519. For instance, ed25519 is known for its speed and resistance to certain types of cryptographic attacks, making it a popular choice for newer blockchains seeking to optimize performance and security.
- Some L1 chains have adopted cryptographic protocols that include additional features, such as zero-knowledge proofs for enhanced privacy, or different hashing algorithms that may be better suited to their specific network requirements.
- The ST33 chip's ECC co-processor is designed to be adaptable, with the capability to support multiple curves and cryptographic protocols. This ensures that SIM3 hardware wallets can cater to the diverse and evolving landscape of L1 blockchains, facilitating secure and efficient operations across various cryptocurrency platforms.

RSA for Broad Cryptographic Applications

- RSA Algorithm: While not directly tied to a specific blockchain, the RSA capabilities of the ST33 are crucial for secure communications and data encryption across various blockchain networks. RSA's widespread acceptance and robustness make it an essential part of the cryptographic toolkit for blockchain applications.

Symmetric Key Algorithms for Encrypted Data Storage

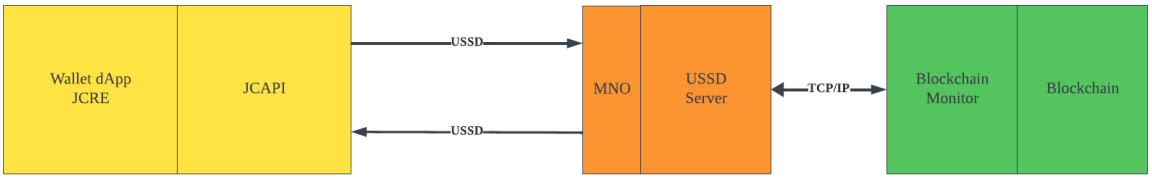
- DES, 3DES, and AES: These symmetric key algorithms are employed for encrypting data stored on the SIM3 card, ensuring the privacy and security of user information. While these algorithms are not used directly in transaction signing for blockchains, they play a vital role in securing the user's data at rest.

Security and Efficiency

- The use of these specific cryptographic algorithms, matched to the requirements of each blockchain, ensures that the SIM3 hardware wallet provides the highest levels of security and operational efficiency. This approach allows users to confidently manage their digital assets across a range of blockchain networks.

SIM3 Data Transmission

Upon the secure signing of a transaction by the SIM3 hardware wallet's applet, the data must be prepared for transmission over the mobile network. Given the limitation in data size for USSD messages, the signed transaction is algorithmically split into manageable blocks. This segmentation is crucial for conforming to the USSD protocol, which was not originally designed for high-volume data transfer.



Modulation and Demodulation Techniques in SIM3 Data Transmission

The SIM3 hardware wallet utilizes a sophisticated modulation technique to encode transaction data into a format suitable for USSD transmission. This technique is critical for overcoming the inherent limitations associated with USSD's narrow data payload capacity and unordered nature of message delivery.

Modulation Process

- During modulation, each data block from the signed transaction is encoded with sequential identifiers and checksums. The sequential identifiers act as indices to maintain the correct order of data blocks, while checksums are integrated using error-detecting codes, such as cyclic redundancy check (CRC), to validate the integrity of each block upon reception. The encoded data blocks are then mapped to the frequency spectrum allocated for USSD communication, a process which may employ techniques like Quadrature Amplitude Modulation (QAM) or Phase Shift Keying (PSK), adapted for the digital signal processing capabilities of the mobile network.

Demodulation at USSD Server

- Once received by the USSD server, the demodulation process begins. The server employs a decoding algorithm that interprets the frequency-encoded data, extracting the sequential identifiers and conducting integrity checks using the embedded checksums. The error-detecting codes allow the server to identify any blocks that may have been corrupted or lost during transmission, triggering error-handling protocols or retransmission requests as necessary.

Reassembly of Transaction Blocks

- The demodulation process includes the reassembly of the ordered data blocks into the original transaction structure. This reassembly is sensitive to the sequencing information, ensuring that each block is restored to its correct position within the transaction. The server then conducts a final integrity check against the entire transaction data, comparing it against a master checksum generated at the modulation stage.

Error Correction and Data Integrity

- To further enhance the reliability of the data transmission, the demodulation algorithm incorporates error correction codes (ECC) using the Turbo Codes, which enable the recovery of the original data even in the event of transmission errors. This forward error correction (FEC) is essential for maintaining data integrity in the variable conditions of mobile network communication.

Error Detection and Integrity Assurance

A critical component of the demodulation process is the verification of data integrity. The USSD server employs a cyclic redundancy check (CRC) to detect any alterations or errors in the transmitted data blocks. The CRC algorithm generates a polynomial code representation of the data block, which can be expressed by the following mathematical equation:

$$CRC(x) = Data(x) \cdot x^n \mod P(x)$$

Where:

- CRC(x) is the resulting CRC code.
- Data(x) represents the data block expressed as a polynomial.
- x(n) indicates the data is multiplied by (x) raised to the power of (n), where (n) is the degree of the generator polynomial P(x).
- P(x) is the generator polynomial predefined for the particular CRC standard used.

Upon reception, the USSD server recalculates the CRC using the received data and compares it to the transmitted CRC code. If the two codes match, the data block is deemed intact. If there is a discrepancy, it indicates that the data block has been corrupted during transmission.
The integrity of the entire transaction is thus ensured through this rigorous error-checking protocol, which is vital for maintaining the fidelity of blockchain communications facilitated by the SIM3 platform.

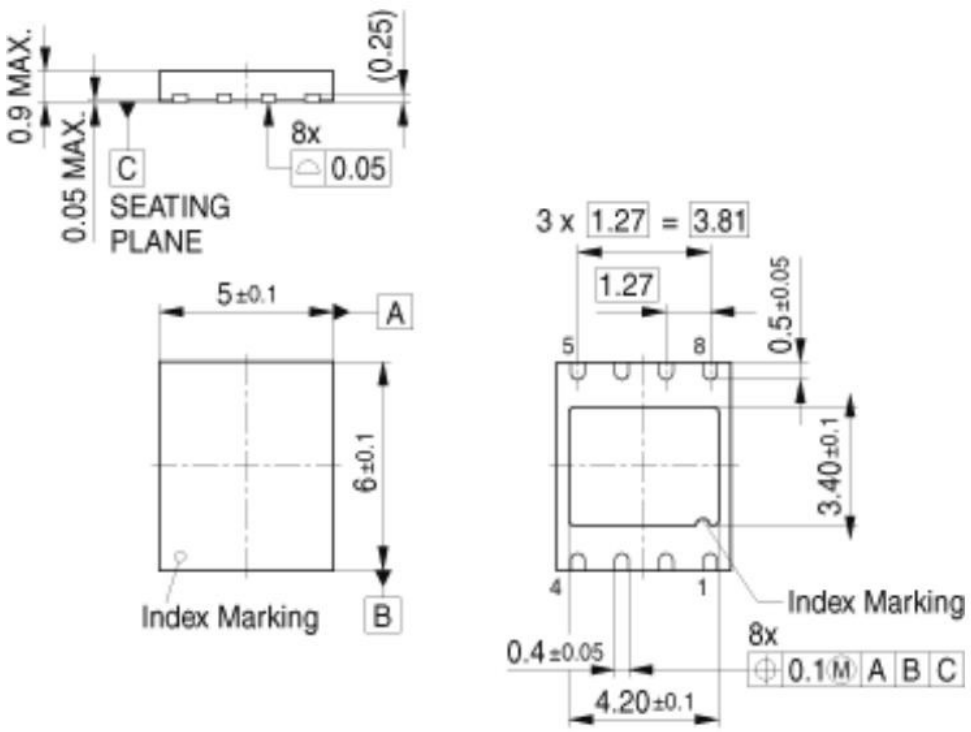
The integrity of the entire transaction is thus ensured through this rigorous error-checking protocol, which is vital for maintaining the fidelity of blockchain communications facilitated by the SIM3 platform.

SIM3 Hardware Product Details

Package handling Description

Our SIM3 module encapsulates cutting-edge technology in two package formats: the 56 DFN and the 2.52.7 WLCSP. The dual packaging options offer flexibility for different device requirements and manufacturing processes.

- Package outline for 5*6 DFN
  - 5*6 DFN: Optimized for robustness and compatibility, the 5*6 DFN package meets the MFF2 standards defined in ETSI TS 102 67, ensuring high interoperability and reliability for embedded mobile applications.

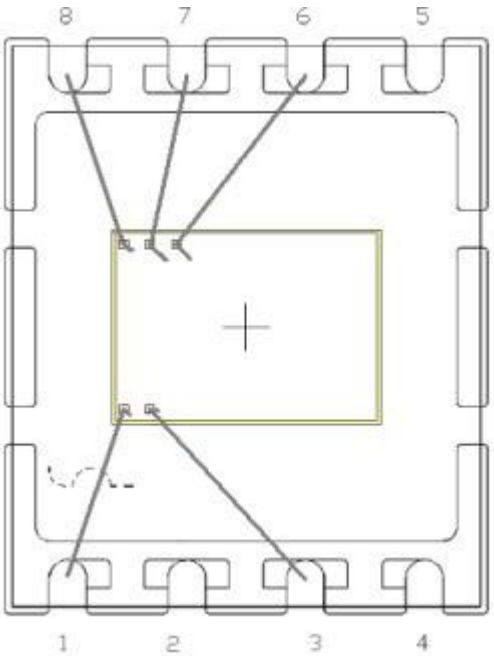


- Manufacturing Compliance
  - The package outline conforms to industry manufacturing standards, providing assurances of mechanical durability and thermal stability. The design accommodates thermal expansion and contraction, preventing physical stress that could lead to component failure. Additionally, the package is designed to withstand the rigors of reflow soldering processes, a testament to its suitability for high-volume production environments.

- Environmental Considerations
  - The materials selected for the 5x6 DFN package are chosen for their low environmental impact and compliance with RoHS regulations. The package is resistant to moisture absorption, reducing the risk of damage during temperature and humidity fluctuations that are common in global logistics and deployment.

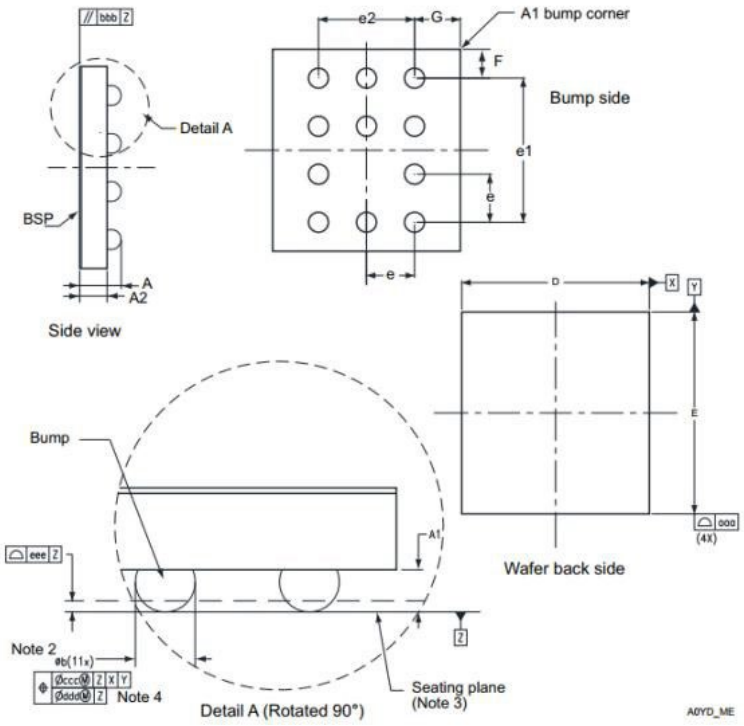
- PIN-out Assignment for 5*6 DFN
  - SIM3's physical connectivity is designed to ensure robust performance and compatibility across a range of mobile devices. Adhering to the MFF2 standard, as defined in ETSI TS 102 67, the SIM3 features a 5*6 Dual Flat No-leads (DFN) package that aligns with the stringent requirements for embedded SIMs in the modern landscape of machine-to-machine communication.

  - Compliance with ETSI TS 102 67: Our commitment to industry standards is evident in our compliance with the MFF2 definition, ensuring that the SIM3 seamlessly integrates into the existing telecommunications infrastructure. This compliance not only facilitates a high level of interoperability but also underscores the reliability and future-proof nature of the SIM3.



PIN	UICC contact	Name	description
1	C5	GND	**Ground**
3	C7	I/O	**Serial data in/output**
6	C3	CLK	**External clock input**
7	C2	RST	**System reset input**
8	**C1**	**VCC**	**Power input**

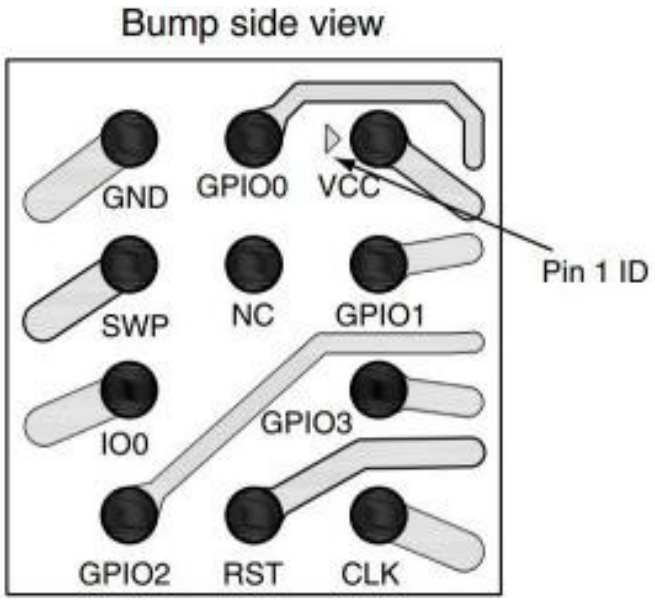
- Package outline for 2.5*2.7 WLCSP
    - 2.5*2.7 WLCSP: This package boasts an ultra-compact footprint with a meticulously organized array of solder bumps, designed to provide a comprehensive suite of electrical connections vital for the module's operation within the mobile ecosystem.



Symbol				
	Min	Typ.	Max.	Unit
A	-	-	0.600	mm
A1	-	0.190	-	mm
A2	-	-	0.395	mm
b	-	0.270	-	mm
D	-	2.539	2.565	mm
E	-	2.735	2.760	mm
e	-	0.650	-	mm
e1	-	1.950	-	mm
F	-	0.393	-	mm
G	-	0.620	-	mm
N(1)	-	11	-	mm
aaa	-	0.110	-	mm
bbb	-	0.110	-	mm
ccc	-	0.110	-	mm
ddd	-	0.060	-	mm
eee	-	0.060	-	mm

- PIN-out Assignment for 2.5*2.7 WLCSP

- The SIM3 module is equipped with a meticulously organized 2.5x2.7 WLCSP (Wafer-Level Chip-Scale Package), featuring an array of solder bumps arranged to provide a comprehensive suite of electrical connections. Each bump is designated for a specific function, crucial for the module's operation within the mobile ecosystem.

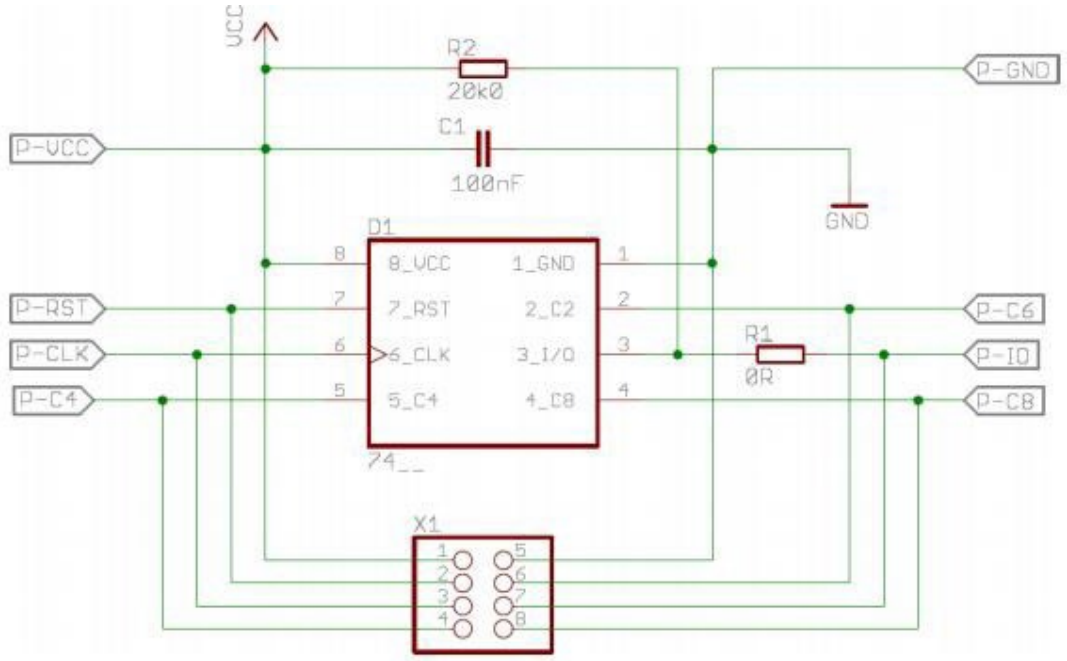


Item	UICC contact	Name	description
1	C5	GND	**Ground**
2	C6	SWP	**Single wire protocol in/output**
3	C7	I/O	**Serial data in/output**
4	-	GPIO2	**General-purpose in/output**
5	-	GPIO0	**General-purpose in/output**
6	-	NC	**No connection**
7	C2	RST	**System reset input**
8	C1	VCC	**Power input**
9	-	GPIO1	**General-purpose in/output**
10	-	GPIO3	**General-purpose in/output**
11	**C3**	**CLK**	**External clock input**

Electrical Specification

Symbol	Description	Minimum	Maximum	Unit	Comment
V(cc)	**Input Supply voltage range**	**-0.3**	**6.5**	**V**	**/**
V(in)	**Input voltage range**	**-0.3**	**V(cc) + 0.3**	**V**	**/**
T(A)	**Operational temperature**	**-30**	**+85**	**C**	**/**
V(ESD)	**ESD Protection**	**4000**	**/**	**V**	**HBM (Human Body Model) JESD22-A114**

Maximum Ratings



Electrical Characteristics

Symbol	Description	Minimum	Norminal	Maximum	Unit	Comment
V(cc)	Input supply voltage range	4.5	5.0	5.5	V	ISO 7816-3 Class A Acc. ETSI 102 671 voltage class A shall not be used
		2.7	3.0	3.3	V	ISO 7816-3 Class B
		1.62	1.8	1.98	V	ISO 7816-3 Class C
I(cc)	Input supply current	/	/	20	mA	25c
I(cc Spike)	Spikes on input supply current	/	/	100	mA	ISO 7816-3 Class A Max. charge: 20 nAS
		/	/	50	mA	ISO 7816-3 Class B Max. charge: 10 nAS
		/	/	30	mA	ISO 7816-3 Class C Max. charge: 6 nAS
I(cc Max)	Current limitation mode: Supply current	/	/	10	mA	Vcc < 5.0V
		/	/	6	mA	Vcc < 3.3V
		/	/	4	mA	Vcc < 1.98V
I(cc S1)	Sleep mode: Supply current	/	/	200	uA	TA=25c; F(clk)=1MHz
I(cc S2)	Sleep mode: Supply current	/	/	100	uA	Class B / C; T(A)=25c;CLK off

DC Characteristics

Symbol	Description	Minimum	Norminal	Maximum	Unit	Comment
I/O; Bidirectional port						
V(iH)	Input Voltage High	0.8 * V(cc)	/	V(cc) + 0.3	V	-20uA <= I(iH) <= 20uA
V(iL)	Input Voltage Low	-0.3	/	0.2 * V(cc)	V	-1mA <= I(iL) <= 20uA
V(oH)	Output Voltage High	0.7 * V(cc)	/	V(cc) + 0.33	V	-20uA <= I(oH) <= 20uA
RST						
V(iH)	Input Voltage High	0.8 * V(cc)	/	V(cc) + 0.3	V	-20uA <= I(iH) <= 20uA
V(iL)	Input Voltage Low	-0.3	/	0.2 * V(cc)	V	-50uA <= I(iL) <= 20uA
CLK						
V(iH)	Input Voltage High	0.85 * V(cc)	/	V(cc) + 0.3	V	-20uA <= I(iH) <= 20uA
V(iL)	Input Voltage Low	-0.3	/	0.2 * V(cc)	V	-30uA <= I(iL) <= 20uA

Electrical for Communication PIN

Contacts	Symbol	Minimum	Norminal	Maximum	Unit	Comment
ISO/IEC 7816-3, 2001						
IO	**V(oL)**	**/**	**/**	**0.15 * V(cc)**	**V**	**Class A: I(oL) = 1mA**
		/	**/**	**0.15 * V(cc)**	**V**	**Class B: I(oL) = 1mA**
		/	**/**	**0.15 * V(cc)**	**V**	**Class C: I(oL) = 500uA**
GSM 11.11 (08-2000); GSM 11.12 (03-1998); GSM 11.18 (07-1999); ETSI TS 102 221 4.3.0 (07-2001)						
IO	**V(oL)**	**/**	**/**	**0.3**	**V**	**Class A & B: I(oL) = -1mA**
		/	**/**	**0.4**	**V**	**Class C: I(oL) = -1mA**
EMV 2000 (Status: 2001-11-30 – Draft Version 1.0)						
IO	**V(oL)**	**/**	**/**	**0.08 * V(cc)**	**V**	**Class A: I(oL) = 1mA**
		/	**/**	**0.15 * V(cc)**	**V**	**Class B: I(oL) = 500uA**
		/	**/**	**0.15 * V(cc)**	**V**	**Class C: I(oL) = 500uA**

Electrical for IO PIN

Symbol	Description	Minimum	Norminal	Maximum	Unit	Comment
V(cc) – Input supply voltage						
t(R_vcc)	**Rise time V(cc)**	**1**	**/**	**10(7)**	**uS**	**0 to 100% of supply voltage**
I/O						
t(R);t(F)	**Rise / Fall time**	**/**	**/**	**1**	**uS**	**30 pF external**
RST						
t(R);t(F)	**Rise / Fall time**	**/**	**/**	**1**	**uS**	**30 pF external**
CLK						
f(CLK)	**External frequency**	**1**	**/**	**10**	**MHz**	
t(R);t(F)	**Rise / Fall time**	**/**	**/**	**0.1 * 1f(aK)**	**ns**	**0.1 * V(cc) to 0.9 * V(cc);V(t)=0.5*V(cc)**
Duty Cycle		**40**	**/**	**60**	**%**	

AC Characteristics

Jellyfish MOBILE

Hardware Information

Technology	80nm CMOS
Cryptography Coprocessor Support	PKI, RSA, ECC, DES, 3DES, AES
Supply Voltage	Class A (5.0V), B (3.0V), C(1.8V)
Operational Temperature	-35c to 85c
Enhanced NVM	NVM write/erase cycles min. 200k per page
	NVM data retention min. 10 years
Certification / Compliance	ETSI 102 221

Other Physical Characteristics

Testing item	Testing method	Result
Antistatic	Withstand ± 4000V contact discharge and ± 8000 non-contact discharge, the electrical characteristics meet the card standard requirements	**PASS**
Vibration test	f(Hz) PSD(g2/Hz) 8 0.5 40 0.1 50 0.3 70 0.3 200 0.03 500 0.01 X、Y、Z axis keep 30 min After testing, Normal operation after power-on, no damage on the card appearance	**PASS**
Impact test	In three mutually perpendicular axes Acceleration: 5000m / S Pulse width: 1ms Frequency: 10 times in each direction Waveform: Semi-positive black wave After the test, the power is working normally, and the appearance is not damaged	**pass**
Humidity test	**The samples were kept at a temperature of 50 C °± 2 C ° and a relative humidity of 93% ± 3%, and 10 samples were kept for 172 hours. After the test, the sample is powered on, working normally, and the appearance is not damaged**	**PASS**

Key standard compliances

Sun/Oracle Specifications

- JCRE 3.0.4 Runtime Environment Specifications, Java Classic Edition Card Platform
- JCVM 3.0.4 Virtual Machine Specification, Java Card Platform, Classic Edition
- JCAPI 3.0.4 Application Programming Interface, Java Card Platform, Classic Edition

GlobalPlatform Specifications

- GlobalPlatform Card Specification, V2.2.1
- GP 2.2 AmdA Confidential Card Content Management
- GP 2.2 AmdB Remote Application Management over HTTP
- GP 2.2 AmdC Contactless Services
- GP 2.2 AmdD Secure Channel Protocol 03
- GP 2.2 AmdE Security Upgrade for Card Content Management
- GP Java Card API
- GP Java Card Contactless API for Card Specification V2.2.1

ETSI

- 102 221 UICC-Terminal interface; physical and logical characteristics
- 102 222 Administrative commands for telecommunications applications
- 102 223 Card Application Toolkit (CAT)
- 102 225 Secured packet structure for UICC based applications
- 102 226 Remote APDU structure for UICC based applications
- 102 241 UICC Application Programming Interface {API) for Java Card
- 102 613 UICC - CLF Interface; Part 1: physical and data link layer characteristics
- 102 622 UICC - CLF Interface; Host Controller Interface (HCI)
- 102 705 UICC Application Programming Interface for Java Card for Contactless Applications

3GPP

- 43.019 Subscriber Identity Module Application Programming Interface (SIM API) for Java Card Stage 2
- 51.011 Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
- 51.014 Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
- 31.048 Security mechanisms for the (U)SIM application toolkit; Test specification
- 31.101 UICC-Terminal Interface; Physical and Logical Characteristics
- 31.102 Characteristics of the USIM Application
- 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application
- 31.111 USIM Application Toolkit (USAT)
- 31.115 Secured packet structure for (U)SIM Toolkit applications
- 31.116Remote APDU Structure for (U)SIM Toolkit applications
- 31.130 (U)SI M API for Java Card
- 31.133 ISIM API for Java Card
- 31.919 2G/3G Java Card API based applet internet working

3GPP2

- C.S0023-C Removable User Identity Module for Spread Spectrum Systems, Rev D VI.0
- C.S0035 CDMA Card Application Toolkit (CCAT), Rev A VI.0
- C.S0065-A cdma2000 Application on UICC for Spread Spectrum Systems, Rev B V2.0

Conclusion

The technical exploration within this document has delineated the comprehensive cryptographic processes that underpin the SIM3 hardware wallet's operations. We have detailed the implementation of ECC, RSA, and symmetric key algorithms like DES, 3DES, and AES, which are integral to the secure generation, storage, and management of cryptographic keys and the execution of blockchain transactions. This cryptographic agility ensures that the SIM3 platform is equipped to handle a diverse array of blockchain protocols, enhancing the user experience in managing digital assets across various networks.

Our platform's design philosophy has been governed by the principles of configurability and flexibility. This approach is manifested in our support for dynamic configuration parameters which optimize the performance of the Java Card Virtual Machine, Runtime Environment, and API layers to suit a wide range of hardware limitations. Such customization capabilities underline the SIM3 platform's readiness to integrate into diverse technological infrastructures and user scenarios.

As we conclude this technical discourse, it is evident that the SIM3 platform is poised to make a significant impact on the telecommunications sector. With its robust architecture and forward-looking design, SIM3 is not merely a response to current market demands but a foundational step towards a future where secure and seamless digital identity and asset management are paramount.

This whitepaper serves as a comprehensive technical record of the SIM3 platform's capabilities and lays the groundwork for its adoption and integration into the broader landscape of mobile connectivity and Web3 services. The innovations presented herein are a testament to Jellyfish Mobile's commitment to advancing the frontier of secure mobile telecommunications technology.