<table>
<tr><th>N</th><th>Field</th><th>Content</th></tr>
<tr><td>0</td><td>Table of Content</td><td>
<table>
<tr><td>00</td><td>Table of Content</td></tr>
<tr><td>01</td><td>Date of Notification</td></tr>
<tr><td>02</td><td>Statement in Accordance with Article 6 (3) of Regulation (EU) 2023/1114</td></tr>
<tr><td>03</td><td>Statement in Accordance with Article 6 (6) of Regulation (EU) 2023/1114</td></tr>
<tr><td>04</td><td>Statement in Accordance with Article 6 (5) points (a), (b), (c) of Regulation (EU) 2023/1114</td></tr>
<tr><td>05</td><td>Statement in Accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114</td></tr>
<tr><td>06</td><td>Statement in Accordance with Article 6(5), points (e) and (f) of Regulation (EU) 2023/1114</td></tr>
<tr><td></td><td>SUMMARY</td></tr>
<tr><td>07</td><td>Warning in Accordance with Article 6(7), Second Subparagraph of Regulation (EU) 2023/1114</td></tr>
<tr><td>08</td><td>Characteristics of the Crypto-Asset</td></tr>
<tr><td>09</td><td>Information about the Quality and Quantity of Goods or Services to which the Utility Tokens Give Access and Restrictions on the Transferability.</td></tr>
<tr><td>10</td><td>Key information about the Admission to Trading</td></tr>
<tr><td></td><td>PART I – INFORMATION ON RISKS</td></tr>
<tr><td>I.01</td><td>Admission to Trading-Related Risks</td></tr>
<tr><td>I.02</td><td>Person Seeking Admission to Trading-Related Risks</td></tr>
<tr><td>I.03</td><td>Crypto-Assets-Related Risks</td></tr>
<tr><td>I.04</td><td>Project Implementation-Related Risks</td></tr>
<tr><td>I.05</td><td>Technology-Related Risks</td></tr>
</table>
</td></tr>
</table>

		I.06	Mitigation Measures	
			PART A – INFORMATION ABOUT THE OFFEROR OR THE PERSON SEEKING ADMISSION TO TRADING	
		A.01	Name	
		A.02	Legal Form	
		A.03	Registered Address	
		A.04	Head Office	
		A.05	Registration Date	
		A.06	Legal Entity Identifier	
		A.07	Another Identifier Required Pursuant to Applicable National Law	
		A.08	Contact Telephone Number	
		A.09	E-mail Address	
		A.10	Response Time (Days)	
		A.11	Parent Company	
		A.12	Members of the Management Body	
		A.13	Business Activity	
		A.14	Parent Company Business Activity	
		A.15	Newly Established	
		A.16	Financial Condition for the Past Three Years	
		A.17	Financial Condition since Registration	
			PART B - INFORMATION ABOUT THE ISSUER, IF DIFFERENT FROM THE OFFEROR OR PERSON SEEKING ADMISSION TO TRADING	
		B.01	Issuer Different from Person Seeking Admission to Trading	
		B.02	Name	
		B.03	Legal Form	
		B.04	Registered Address	
		B.05	Head Office	
		B.06	Registration Date	
		B.07	Legal Entity Identifier	
		B.08	Another Identifier Required Pursuant to Applicable National Law	
		B.09	Parent Company	

		B.10	Members of the Management Body	
		B.11	Business Activity	
		B.12	Parent Company Business Activity	
			PART C – INFORMATION ABOUT THE OPERATOR OF THE TRADING PLATFORM IN CASES WHERE IT DRAWS UP THE CRYPTO-ASSET WHITE PAPER AND INFORMATION ABOUT OTHER PERSONS DRAWING THE CRYPTO-ASSET WHITE PAPER PURSUANT TO ARTICLE 6(1), SECOND SUBPARAGRAPH, OF REGULATION (EU) 2023/1114	
		C.01	Name	
		C.02	Legal Form	
		C.03	Registered Address	
		C.04	Head Office	
		C.05	Registration Date	
		C.06	Legal Entity Identifier of the Operator of the Trading Platform	
		C.07	Another Identifier Required pursuant to Applicable National Law	
		C.08	Parent Company	
		C.09	Reason for Crypto-Asset White Paper Preparation	
		C.10	Members of the Management Body	
		C.11	Operator Business Activity	
		C.12	Parent Company Business Activity	
		C.13	Other Persons Drawing up the Crypto- Asset White Paper According to Article 6(1), Second Subparagraph, of Regulation (EU) 2023/1114	
		C.14	Reason for Drawing the White Paper by Persons Referred to in Article 6(1), Second Subparagraph, of Regulation (EU) 2023/1114	
			PART D – INFORMATION ABOUT THE CRYPTO-ASSET PROJECT	
		D.01	Crypto-Asset Project Name	
		D.02	Crypto-Assets Name	
		D.03	Abbreviation	
		D.04	Crypto-Asset Project Description	
		D.05	Details of all Natural or Legal Persons Involved in the Implementation of the Crypto-Asset Project	
		D.06	Utility Token Classification	
		D.07	Key Features of Goods/Services for Utility Token Project	

			D.08	Plans for the Token	
			D.09	Resource Allocation	
			D.10	Planned Use of Collected Funds or Crypto-Assets	
				PART E – INFORMATION ABOUT THE OFFER OR THE ADMISSION TO TRADING OF THE CRYPTO-ASSET	
			E.01	Admission to Trading	
			E.02	Reasons for the Admission to Trading	
			E.03	Fundraising Target	
			E.04	Minimum Subscription Goals	
			E.05	Maximum Subscription Goals	
			E.06	Oversubscription Acceptance	
			E.07	Oversubscription Allocation	
			E.08	Issue Price	
			E.09	Official Currency or Any Other Crypto-Assets Determining the Issue Price	
			E.10	Subscription Fee	
			E.11	Offer Price Determination Method	
			E.12	Total Number of Traded Crypto-Asset	
			E.13	Targeted Holders	
			E.14	Holder Restrictions	
			E.15	Reimbursement Notice	
			E.16	Refund Mechanism	
			E.17	Refund Timeline	
			E.18	Offer Phases	
			E.19	Early Purchase Discount	
			E.20	Time-Limited Offer	
			E.21	Subscription Period Beginning	
			E.22	Subscription Period End	
			E.23	Safeguarding Arrangements for Offered Funds/Crypto-Assets	

E.24	Payment Methods for Crypto-Asset Purchase		
E.25	Value Transfer Methods for Reimbursement		
E.26	Right of Withdrawal		
E.27	Transfer of Purchased Crypto-Assets		
E.28	Transfer Time Schedule		
E.29	Purchaser's Technical Requirements		
E.30	Crypto-Asset Service Provider (CASP) Name		
E.31	CASP Identifier		
E.32	Placement Form		
E.33	Trading Platforms Name		
E.34	Trading Platforms Market Identifier Code (MIC)		
E.35	Trading Platforms Access		
E.36	Involved Costs		
E.37	Offer Expenses		
E:38	Conflicts of Interest		
E.39	Applicable Law		
E.40	Competent Court		
	PART F – INFORMATION ABOUT THE CRYPTO-ASSET		
F.01	Crypto-Asset Type		
F.02	Crypto-Asset Functionality		
F.03	Planned Application of Functionalities		
F.04	Type of White Paper		
F.05	Type of Submission		
F.06	Crypto-Asset Characteristics		
F.07	Commercial Name or Trading Name		
F.08	Website of the Issuer		
F.09	Starting Date of the Admission to Trading		
F.10	Publication Date		

			F11	Any other Services Provided by the Issuer	
			F.12	Identifier of Operator of the Trading Platform	
			F.13	Language or Languages of the White Paper	
			F.14	Digital Token Identifier Code Used to Uniquely Identify the Crypto-Asset or each of the Several Crypto Assets to which the White Paper Relates, Where Available	
			F.15	Functionally Fungible Group Digital Token Identifier, Where available	
			F.16	Voluntary Data Flag	
			F.17	Personal Data Flag	
			F.18	LEI Eligibility	
			F.19	Home Member State	
			F.20	Host Member States	
				PART G – INFORMATION ON RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS	
			G.01	Purchaser Rights and Obligations	
			G.02	Exercise of Rights and Obligations	
			G.03	Conditions for Modifications of Rights and Obligations	
			G.04	Future Public Offers	
			G.05	Issuer Retained Crypto-Assets	
			G.06	Utility Token Classification	
			G.07	Key Features of Goods/Services of Utility Tokens	
			G.08	Utility Tokens Redemption	
			G.09	Non-Trading Request	
			G.10	Crypto-Assets Purchase or Sale Modalities	
			G.11	Crypto-Assets Transfer Restrictions	
			G.12	Supply Adjustment Protocols	
			G.13	Supply Adjustment Mechanisms	
			G.14	Token Value Protection Schemes	
			G.15	Token Value Protection Schemes Description	
			G.16	Compensation Schemes	

		G.18	Applicable Law
		G.19	Competent Court
			PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY
		H.01	Distributed Ledger Technology
		H.02	Protocols and Technical Standards
		H.03	Technology Used
		H.04	Consensus Mechanism
		H.05	Incentive Mechanisms and Applicable Fees
		H.06	Use of Distributed Ledger Technology
		H.07	DLT Functionality Description
		H.08	Audit
		H.09	Audit Outcome
			PART J – INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS
		J-01	Adverse Impacts on Climate and other Environment-Related Adverse Impacts
		S.01	Name
		S.02	Relevant Legal Entity Identifier
		S.03	Name of the Crypto-Asset
		S.04	Consensus Mechanism
		S.05	Incentive Mechanisms and Applicable Fees
		S.06	Beginning of the Period to which the Disclosure Relates
		S.07	End of the Period to which the Disclosure Relates
		S.08	Energy Consumption
		S.09	Energy Consumption Sources and Methodologies
01	Date of Notification	2025-09-30	

02	Statement in Accordance with Article 6(3) of Regulation (EU) 2023/1114	This White Paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading (“Person Seeking Admission to Trading”) of the crypto-asset is solely responsible for the content of this crypto-asset white paper.
03	Compliance Statement in Accordance with Article 6(6) of Regulation (EU) 2023/1114	This White Paper paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.
04	Statement in Accordance with Article 6(5), points (a), (b), (c) of Regulation (EU) 2023/1114	The crypto asset referred to in this white paper (“Token”) may lose its value in part or in full, may not always be transferable and may not be liquid.
05	Statement in Accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114	The Token may not be exchangeable against the good or service promised in the crypto-asset white paper, especially in the case of a failure or discontinuation of the crypto-asset project.
06	Statement in Accordance with Article 6(5), points (e) and (f) of Regulation (EU) 2023/1114	The Token is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council. The Token is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

SUMMARY		
07	Warning in Accordance with Article 6(7), Second Subparagraph of Regulation (EU) 2023/1114	WARNING This summary should be read as an introduction to the White Paper. The prospective holder should base any decision to purchase this crypto asset on the content of the White Paper as a whole and not on this summary alone. The admission to trading of this Token does not constitute an offer or solicitation to purchase financial instruments, or an admission to trading of financial instruments and any such offer, solicitation, or admission can be made only by means of a prospectus or other offer documents pursuant to the applicable national law. This White Paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.
08	Characteristics of the Crypto-Asset	● The Token is a fungible token issued on the BNBChain and Base blockchain based on the ERC-20 standard. ● The Token has an initial total supply of 1,000,000,000 (one billion) units. ● The Token is designed to serve as the utility token of the zkPass Protocol (“Protocol”). The Protocol is not itself a distributed ledger but operates as a verification layer across multiple distributed ledger systems, including Ethereum and EVM-compatible Layer-2 networks. Deployments on these networks allow the Protocol to act as a decentralized verification oracle, turning private Web2 data into reusable zero-knowledge proofs. This functionality powers a unified “verifiable layer” for applications in finance, identity, education, social reputation, AI, and DePIN. **Utility and Scope of the Service:** The Token provides access to the Protocol’s core utilities, including settlement of proofs, staking for verifiers, incentives for users and developers, and participation in governance over protocol standards

		and treasury flows. All components of the Protocol that involve economic coordination, including proof validation and staking rewards, are managed through Token-based mechanisms executed on-chain. **Governance and Issuer's Role:** Once Tokens are issued, the ongoing evolution of the Protocol is directed through DAO-based governance. Token holders may participate in decisions relating to protocol upgrades, validator incentives, and treasury allocations. Control over these functions rests with Token-based governance rather than the original issuer, IFCONNECT TECHNOLOGY LIMITED. The Token qualifies as a crypto-asset other than an electronic money token or an asset-referenced token, and specifically, as a utility token under Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets ("MiCA").
09	Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	The Token grants holders access to the services of the zkPass Protocol. These services include (i) settlement of zero-knowledge proofs generated through the Protocol, (ii) staking for verifiers and node operators as collateral in the verification process, (iii) incentives and rewards for users, developers and ecosystem partners who generate or consume proofs, and (iv) participation in governance decisions concerning protocol upgrades, standards, and treasury allocations. The Token has a fixed maximum supply of 1,000,000,000 (one billion) units, and no additional issuance beyond this amount is foreseen. Accordingly, access to the above services is limited by the availability of Tokens in circulation, and the economic coordination within the Protocol is designed around this capped supply. The Token is freely transferable on-chain and may be traded on regulated trading venues. However, certain categories of allocations (e.g., team, early investors, community incentives) are subject to contractual vesting or lock-up schedules as defined in the token distribution framework. Aside from these vesting-related restrictions, no technical restrictions are imposed on the transferability of the Token, subject always to applicable laws and regulations in the jurisdictions where it is offered or traded.

10	Key Information about the Admission to Trading	Admission to trading is sought on platforms operating within the European Union ("EU") or the European Economic Area ("EEA") ("Trading Platforms"). In seeking admission to trading, the Person Seeking Admission to Trading complies with its obligations under article 5 of Regulation (EU) 2023/1114. At the time of the present notification, no listing agreement has been entered into with a Trading Platform. The up-to-date list of available Trading Platforms will be made available on the Person Seeking Admission to Trading's website.
PART I – INFORMATION ON THE RISKS		
I.01	Admission to Trading – Related Risks	● **No Listing Risk**: The present white paper is drafted and notified by the Person Seeking Admission to Trading in accordance with its obligations under Article 5 of MiCA, in its capacity as a person seeking the admission of the Token to trading. As of the date of notification, the Person Seeking Admission to Trading has not entered into any listing agreement with any Trading Platforms. The Person Seeking Admission to Trading its affiliates, directors, and officers shall not be held liable for any damages, losses, costs, fines, penalties, or expenses of any kind - whether or not reasonably foreseeable by the Person Seeking Admission to Trading or the Token holder - that the Token holder may suffer, sustain, or incur in connection with, or as a result of, the Token not being listed on a Trading Platform. ● **General Contractual and Counterparty Risk**: The Person Seeking Admission to Trading neither operates nor controls, oversees, or manages the functioning of crypto-asset services providers as defined under MiCA ("CASP") operating within the EU /EEA and Trading Platforms (together with CASPs, the " Exchanges"), where the Token will be admitted for trading or listed. When Token holders buy or sell the Token on Exchanges, the Person Seeking Admission to Trading is not a contractual party to these transactions. As a result, ■ any legal relationship between Token holders and the Exchange is governed solely by the terms and conditions set by each Exchange at its discretion. ■ The Person Seeking Admission to Trading assumes no responsibility or liability for the

		operations, services, security, performance, or any outcomes—whether financial or technical—arising from transactions conducted on these Exchanges. ■ The Person Seeking Admission to Trading provides no assurances regarding any Exchange itself and assumes no responsibility or liability for any regulatory, compliance, operational, financial, technical, or reputational failures that may adversely affect its activities. This includes, but is not limited to, circumstances where such failures result in disruptions, restrictions on trading, or the Exchange halting or ceasing its operations entirely, due to sanctions, bankruptcy or alike. The foregoing may result in substantial or even total losses for the Token holder. ● Pausing and Delisting Risk: The Person Seeking Admission to Trading cannot guarantee that the Token will remain listed or tradeable on any Exchanges. Delisting (or the temporary pausing of such listing) could significantly hinder the ability of Token holders to buy, sell, or otherwise transact in Tokens. In the event of delisting, Token holders may face challenges in finding alternative markets or counterparties willing to trade Tokens, which could adversely impact the Token's liquidity and market value. Delisting could also negatively impact the price of the Token, due to modified demand for the Token and/or reputational impact. ● Trading Risk: The Person Seeking Admission to Trading does not control the secondary markets. There can be no assurance as to the secondary market (if any) in the Tokens, and specifically: ■ it cannot guarantee the depth, stability, or sustainability of any secondary market for Tokens. Limited market depth or trading activity may result in reduced liquidity, increased price volatility, and challenges in buying or selling Tokens at desired prices; and ■ it cannot guarantee the healthy and consistent availability of buying or selling opportunities for Tokens or the integrity of their market price. Trading activity may be affected by manipulative practices such as wash trading, front-running, and similar schemes. While Exchanges are subject to varying regulatory frameworks that may or may not prohibit such practices and impose oversight to detect and deter them, the Person Seeking Admission to Trading assumes no responsibility or liability for their effective prevention or enforcement. ● Unsolicited Admission to Trading Risk: Third parties can elect to support Tokens on their Trading Platforms without any request nor authorization or approval by the Person Seeking Admission to Trading or anyone else. Token integration on any third-party platform does not imply any endorsement by the Person Seeking Admission to Trading that such third-party services are valid, legal, stable or otherwise

		appropriate. ● Operational and Technical Risk: Exchanges operate interfaces that allow users to trade crypto-assets for fiat currencies, such as U.S. Dollars and Euros, or other crypto-assets. The reliance on the Exchange's internal system for asset storage and transfer adds an additional layer of counterparty risk, as users are exposed to potential operational, technical, or human errors during these processes. As a result, the Person Seeking Admission to Trading assumes no responsibility or liability for any losses arising from these risks. ■ Trades on these Exchanges are executed based on a centralized matching algorithm and are often recorded off-chain, meaning they are not directly related to transparent on-chain transfers of crypto-assets, and could dissimulate detrimental trade matching or rogue practices. The traded assets are recorded solely on the Exchange's internal ledger, with each internal ledger entry corresponding to an offsetting trade involving either government currency or another crypto asset. ■ Additionally, funds deposited by users for trading may be co-mingled by the Exchanges, rather than stored in unique wallet addresses for each user. This practice results in the centralization of a large volume of assets in a single location, which in turn increases the potential risk of damage or theft, particularly in the event of a hack or security breach. ■ Furthermore, users who wish to trade or withdraw their Tokens must deposit them into the Exchange, increasing the risk of loss in the event of a failure of the deposit or withdrawal processes set up by the Exchange. ● Unanticipated Risks: In addition to the risks outlined in this Section, unforeseen risks may arise. Additionally, new risks could emerge as unexpected variations or combinations of the risks discussed in these Sections I.1 to I.5.
I.02	Person Seeking Admission to Trading- Related Risks	● **Abandonment / Lack of Success Risk**: This is the risk that the activities of the Person Seeking Admission to Trading and Issuer must be partially or totally abandoned for several reasons including, but not limited to, lack of interest from the public, lack of funding, incapacitation of key developers and project members, force majeure (including pandemics and wars) or lack of commercial success or prospects. ● **Legal and Regulatory Compliance Risk**: Crypto assets and blockchain-based technologies are

		subject to evolving regulatory landscapes worldwide. Regulations vary across jurisdictions and may be subject to significant changes. This could lead to changes with respect to trading of the Token and increase the Person Seeking Admission to Trading and Issuer's costs and/or obligations in admitting the Token for trading. Changes in laws or regulations may negatively impact the value, legality, or functionality of the Token. Non-compliance can result in investigations, enforcement actions, penalties, fines, sanctions, or the prohibition of the trading of the Token impacting its viability and market acceptance. The Person Seeking Admission to Trading and Issuer could also be subject to private litigation. • **Reputational Risk**: The Person Seeking Admission to Trading and Issuer face the risk of negative publicity, whether due, without limitation, to operational failures, security breaches, or illicit activities, all of which can damage the Person Seeking Admission to Trading/Issuer's reputation and, by extension, the value and acceptance of the Token. • **Key Individuals Risk**: The success of a crypto projects can be highly dependent on the expertise and leadership of key individuals. Loss or changes in the Person Seeking Admission to Trading and Issuer's leadership could lead to disruptions, loss of trust, or project failure. • **Internal Control Risk**: Any failure by the Person Seeking Admission to Trading and Issuer to develop or maintain effective internal controls or any difficulties encountered in the implementation of such controls, or their improvement could harm it, causing the issuer to have to report such failures. Such failures could lead to a loss of trust and further harm the business of the Person Seeking Admission to Trading and Issuer, causing disruptions, financial losses, or reputational damage affecting the Token. Fraudulent activity or mismanagement by the Person Seeking Admission to Trading and Issuer could directly impact the usability or value of the Token or damage the credibility of the Protocol and the project at broad. • **Unanticipated Risks**: In addition to the risks outlined in this Section, unforeseen risks may arise. Additionally, new risks could emerge as unexpected variations or combinations of the risks discussed in these Sections I.1 to I.5.
I.03	Crypto-Assets-Related Risks	• **Token Admission to Trading "As Is" Risk**: The Tokens are admitted to trading on an "as is" and "as available" basis without warranties of any kind, and the Person Seeking Admission to Trading and Issuer expressly disclaim all implied warranties that the Token, the software code of the programs, are free of viruses or other harmful components which may affect the Tokens.

		• **Decentralized Governance Risk**: The smart contracts governing the Tokens operate under decentralized, on-chain governance (see Sections 08 and F.02). Consequently, the original issuer no longer has control over the Tokens, including their attributes, functionality, and utility. Token holders collectively make decisions about such smart contract and the Protocol at broad, which may result in changes to the token and its features. These could include, but are not limited to, modifications to economic parameters (such as implementing inflationary or deflationary mechanisms), the introduction of new functionalities, or adjustments to the governance structure. • **Market Risk:** Crypto assets, including Tokens, are highly volatile and can experience significant price swings in short periods, increasing the risk of sudden and substantial losses. Such valuation risk arises as the market value of a crypto asset may not always reflect its underlying utility or fundamentals and is subject to subjective assessment. Token holders are thus exposed to potential for losses due to the Token's ▪ potential fluctuations in value, driven by various factors such as supply and demand dynamics, investor sentiment, and broader market trends, incl. changes in interest rates, general movements in local and international markets, technological advancements, regulatory changes, and media coverage. Notably, momentum pricing of crypto assets has previously resulted, and may continue to result, in speculation regarding future appreciation or depreciation in the value of such assets, further contributing to volatility and potentially inflating prices at any given time. ▪ liquidity risk, where a lack of depth in secondary markets – if any – or limited trading volumes can hinder the ability to execute trades at favorable prices, which could lead to significant losses, especially in fast-moving market conditions. As a result, holders of Tokens may experience challenges in managing their holdings, with the value of the asset subject to unpredictable fluctuations and potential depreciation. ▪ solvency and collateral risk, if the Token is used to finance further activities, especially in leveraged positions or as collateral for loans. Significant fluctuations in the value of the Token could adversely affect the solvency of its holder, particularly if the Token is pledged as collateral. A drastic decline in its value may trigger margin calls or automatic liquidations, which could further depress the Token's price, creating a negative feedback loop. This volatility poses the risk of forced asset sales, potentially resulting in substantial losses for the holder and amplifying downward pressure on the market price of Tokens.

		• **Custodial Risk.** The method chosen to store Tokens, like any crypto-asset, carries inherent risks related to the security and management of the storage solution. The chosen storage method—whether hot or cold wallets, or centralized custody—can significantly impact the safety, liquidity, and accessibility of Tokens, with direct consequences for the holder's ability to access, trade, or retain their assets. • **Scam Risk.** This is the risk of loss resulting from a scam or fraud suffered by Token holders from other malicious actors. These scams include, but are not limited to, phishing on social Platforms or by email, fake giveaways, identity theft, creation of fake Tokens, offering fake Token airdrops, among others. • **Anti-Money Laundering/Counter-Terrorism Financing Risk:** This is the risk that crypto-asset wallets holding Token or transactions in Token may be used for money laundering or terrorist financing purposes or identified to a person known to have committed such offenses. There is thus a risk that a public address holding Tokens could be flagged in relation to Anti-Money Laundering or Counter-Terrorism Financing efforts. In such cases, receiving Tokens could result in the holder's address being flagged by relevant authorities, Trading Platforms, or other service providers, which may lead to restrictions on transactions or the freezing of assets. Consequently, holders of Tokens may face legal or regulatory challenges if their address becomes associated with illicit activities, impacting their ability to freely access, trade, or transfer their Tokens. • **Taxation Risk:** The taxation regime that applies to the trading of Tokens by either individual holders or legal entities will depend on each Token holder's jurisdiction. The Person Seeking Admission to Trading cannot guarantee that the holding of Tokens, the reception of the Token, conversions of fiat currency against Tokens, or conversions of other crypto assets against Tokens, will not incur tax consequences. It is the Token holder's sole responsibility to comply with all applicable tax laws, including, but not limited to, the reporting and payment of income tax, wealth tax or similar taxes arising in connection with the appreciation and depreciation of the Token. • **Market Abuse Risk:** The market for crypto assets is rapidly evolving, spanning local, national, and international platforms with an expanding range of assets and participants. Any market abuse, along with a potential loss of confidence among holders, could adversely impact the value and stability of Tokens, and by extension the trading conditions on the Trading Platforms. Notably, ▪ significant trading activity may take place on systems and platforms with limited oversight and predictability. Sudden and rapid changes in the supply or demand of a crypto asset, particularly those with low market capitalization or low unit prices, can result in extreme price volatility.

		▪ the inherent characteristics of crypto assets and their underlying infrastructure may be exploited by certain market participants to engage in abusive trading practices such as front-running, spoofing, pump-and-dump schemes, and fraud across different platforms, systems, or jurisdictions. ● **Legal and Regulatory Risk:** There is a lack of regulatory harmonization and cohesion globally, which results in diverging regulatory frameworks and possible further regulatory evolutions in the future. These could negatively impact the value, utility, and overall viability of Tokens and, in extreme cases, force the Person Seeking Admission to Trading to cease operations. Notably, ▪ while Tokens do not create or confer any contractual or other obligations against any party, certain non-EU regulators may nevertheless classify them as securities, financial instruments, or payment instruments under their respective legal frameworks. Such classifications could impose specific regulatory constraints, leading to significant changes in how Tokens are structured, issued, purchased, or traded. ▪ Evolving regulations could substantially increase the Person's Seeking Admission to Trading compliance costs and operational burdens related to facilitating transactions in Tokens. ▪ New or restrictive regulations could result in the Token losing functionality, depreciating in value, or even becoming illegal or impossible to use, buy, or sell in certain jurisdictions. ▪ Regulators could take enforcement action against the Person Seeking Admission to Trading if they determine that the Token constitutes a regulated instrument or that the Person Seeking Admission to Trading's activities violate existing laws. Such actions could expose the Person Seeking Admission to Trading, its affiliates, directors, and officers to legal and financial penalties, including civil and criminal liability. ● **Unanticipated Risks:** In addition to the risks outlined in this Section, unforeseen risks may arise. Additionally, new risks could emerge as unexpected variations or combinations of the risks discussed in these Sections I.1 to I.5.
I.04	Project Implementation-Related Risks	● **Protocol "As Is" Risk:** The Protocol is and any future components will be deployed on an "as is" and "as available" basis without warranties of any kind, and the Person Seeking Admission to Trading expressly disclaims all implied warranties as to the Protocol and the Token including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. Therefore,

		the Person Seeking Admission to Trading cannot and does not warrant that the Token, the programs, or the technology underlying the Tokens or the Protocol (jointly, "zkPass **Technology**") are reliable, current or error-free, free of viruses or other harmful components, meet the Token's requirements, or that defects in the zkPass Technology will be corrected. Additionally, due to the decentralized nature of the Protocol, there is a risk that functionalities intended to be unlocked may be abandoned, that no new functionalities may be added, and that the Person Seeking Admission to Trading has no influence or control over such developments. ● **Decentralized Governance and Protocol Change Risk:** The Protocol operates under decentralized, on-chain governance (see Sections 08 and F.02). Token holders collectively make decisions about the Protocol, which may result in changes to its functionality and features. These could include, but are not limited to, modifications to economic parameters, the introduction of new functionalities, or adjustments to the governance structure. The Protocol accessible through the Token may develop over time, potentially resulting in significant changes to its initial goals or the methods by which those goals are pursued. While such evolution can promote innovation and strengthen adaptability, it also presents certain risks, such as alterations in the value proposition and possible divergence from stakeholders' previous expectations. ● **Novel Ecosystem Risk:** The Token holder understands and acknowledges that the zkPass ecosystem, as evolving around the Protocol, is built on emerging and rapidly evolving technologies, which inherently carry significant risks. The underlying software, blockchain infrastructure, smart contracts, and related technologies are still in their early stages of development, meaning there is no guarantee that the process of receiving, using, or holding Tokens will be uninterrupted or error-free. As with any novel technology stack, there is an inherent risk that the underlying blockchain, smart contracts, or associated components may contain weaknesses, vulnerabilities, or bugs, despite audits being conducted. Such issues could lead to unintended behaviors, security breaches, or critical failures, potentially resulting in the partial or complete loss of Tokens or their functionality. Additionally, unforeseen technical limitations, incompatibilities, or the emergence of superior alternatives could further impact the stability, security, and long-term viability of the zkPass ecosystem. ● **Industry and Competition Risk:** The project is and will be subject to all the risks and uncertainties associated with any new venture, visionary projects, including the risk that the project cannot be realized in line with its original purpose or vision about the Protocol. Other projects may have the same or a similar vision as the projects There are several other crypto-assets and projects, and new competitors may enter the market at any time. The effect of new or additional competition on the Token or its market price cannot be predicted or quantified. Competitors may have significantly greater financial and legal resources than

		the project and there is no guarantee that the project will be able to compete successfully, or at all, with such competitors. Moreover, increased competition may severely impact the profitability and creditworthiness of the project and involved entities. ● **Dependency/Withdrawing Partners Risk:** The Protocol relies on third-party technologies, infrastructures, and protocols, which could impact its functionality, security, and long-term sustainability. Loss or changes in the key partners providing such technologies can lead to disruptions, loss of trust, or project failure. Any disruptions, vulnerabilities, regulatory scrutiny, or changes in operation of third- party technologies (such as modifications to its mechanisms, governance, or economic incentives) could directly affect the usability and security of the Protocol, which may result in a negative effect for the Tokens. If the third-party technologies experiences technical failures, security breaches, or regulatory intervention, it could severely impact the stability and performance of the Protocol, potentially limiting its intended functionality and value. This reliance on external infrastructure increases systemic risk, as unforeseen issues in third-party protocols could cascade into disruptions within the Token ecosystem. ● **Withdrawing Partners Risk:** This is the risk that the Person Seeking Admission to Trading faces in its business relationships with one or more third parties. The implementation of the Protocol depends strongly on the collaboration and functioning of services provided by several third parties and other crucial partners. The Person Seeking Admission to Trading cannot guarantee that the Protocol and the related project will be successfully developed and deployed. ● **Unanticipated Risks**: In addition to the risks outlined in this Section, unforeseen risks may arise. Additionally, new risks could emerge as unexpected variations or combinations of the risks discussed in these Sections I.1 to I.5
I.05	Technology-Related Risks	The Person Seeking Admission to Trading and its affiliate, directors and officers shall not be responsible or liable for any damages, losses, costs, fines, penalties or expenses of whatever nature, whether reasonably foreseeable by them and the Token holder, and which the Token holder, may suffer, sustain, or incur, arising out of or relating to the technical risks outlined below or a combination thereof. ● **General Cybercrime Risk:** The Token holder acknowledges that, despite best efforts to enhance security, the technological components supporting the Token—including its blockchain infrastructure, smart contracts, wallets—may be vulnerable to cyberattacks. Malicious actors may exploit software vulnerabilities, attack consensus mechanisms, or compromise private keys to gain unauthorized access to Tokens. Risks include hacking attempts on the Protocol, smart contract exploits, phishing attacks, malware infections, and other forms of cybercrime that could result in the theft, loss, or unauthorized

transfer of Tokens. Since digital assets exist entirely in a technological environment, they are inherently exposed to evolving cyber threats, some of which may be undetectable or irreparable until after significant damage has occurred.

- **Blockchain-Level Risk:** The Token holder understands and accepts that, as with other blockchains, the blockchain used for the issuance of the Tokens could be susceptible to consensus-related attacks, including but not limited to double-spend attacks, majority validation power attacks, censorship attacks, and byzantine behavior in the consensus algorithm or be subject to forks. Any successful attack or fork presents a risk to the Token, the expected proper execution and sequencing of Token-transactions and the expected proper execution and sequencing of contract computations as well as the Token balances in the wallet of the Token holders.

- **Smart Contract-Level Risk:** The issuance and transfers of Tokens rely on smart contracts deployed on a blockchain Protocol, which introduce specific technical and security risks.

  - Smart contracts are self-executing, meaning any vulnerabilities, coding errors, or unforeseen logic flaws in the issuance contract could result in unintended consequences, such as the incorrect distribution of Tokens, loss of funds, or permanent locking of Tokens. Additionally, smart contracts are exposed to potential exploits, including hacking attempts, reentrancy attacks, and other forms of malicious activity that could compromise the security of the issuance process.

  - Once deployed, the smart contract governing the issuance of Tokens cannot be easily altered or corrected, meaning any discovered vulnerabilities may be difficult or impossible to fix without significant coordination, community approval, or even a Protocol fork. Furthermore, changes to the underlying blockchain protocol—such as updates to consensus mechanisms, transaction processing rules, or gas fee structures—could affect the functionality or cost-efficiency of the issuance smart contract. These risks could lead to disruptions in Token issuance, security breaches, or a loss of confidence in the zkPass ecosystem, potentially impacting the Token's value and usability.

- **Protocol-Level Risk:** It cannot be excluded that any technical failure, malfunction, or vulnerability within the Protocol could directly or indirectly impact the value of the Token.

  - The Protocol could be subject to critical exploits, such as reentrancy attacks, logic errors, or oracle manipulation, which could lead to unintended Token transfers, assets being drained from the system, or Tokens being irretrievably lost. Fixing such issues may require significant coordination, governance approval, or even disruptive measures such as protocol migrations or forks,

		none of which are guaranteed to be successful. ■ Because the Token's value is inherently tied to its governance functionality, any security breach, or governance deadlock affecting the Protocol or the decentralized governance system could have cascading effects, including depreciation of the Token's value, reduced market confidence, and potential loss of funds for Token holders. ● **Finality or Irrevocability of Transactions**: There is a risk that transactions may be irreversible, depending on the tools and service providers used to initiate them. Access to and any claim on such transactions could be lost indefinitely or permanently. For example, this could occur if (i) a blockchain address is entered incorrectly and the true owner is never identified, (ii) the private key associated with the address is lost, (iii) the address belongs to an entity that will not return the crypto asset, or (iv) the address belongs to an entity that may return the asset but requires additional actions, such as identity verification. ● **Unanticipated Risks**: In addition to the risks outlined in this Section, unforeseen risks may arise. Additionally, new risks could emerge as unexpected variations or combinations of the risks discussed in these Sections I.1 to I.5.
I.06	Mitigation Measures	Various measures to mitigate the risks outlined in Sections I.01 to I.05 above have been implemented. These include rigorous technology testing and auditing, and the careful selection of personnel, management, and third- party partners. However, many of these risks are inherent to the activities with crypto assets and the broader ecosystem, making complete elimination impossible. To further reduce exposure to these risks, prospective Token holders should adopt appropriate safeguards based on their chosen custody method and remain vigilant by actively monitoring publicly available news and market signals, enabling them to respond swiftly to significant developments which may result in the materialization of specific risks.
PART A – INFORMATION ABOUT THE PERSON SEEKING ADMISSION TO TRADING		
A.01	Name	zkPass DAO

A.02	Legal Form	Not-for-profit Association (Verein) incorporated under Articles 60 et seq. of the Swiss Civil Code.
A.03	Registered Address	Zug, Switzerland
A.04	Head Office	Not applicable.
A.05	Registration Date	April 13, 2024
A.06	Legal Entity Identifier	Not applicable.
A.07	Another Identifier Required Pursuant to Applicable National Law	Not applicable.
A.08	Contact Telephone Number	+1 (817) 971-9252
A.09	E-Mail Address	info@zkpass.org
A.10	Response Time (Days)	Within up to 30 calendar days, depending on the time of year and the complexity of the request.

A.11	Parent Company	None (the issuer is an independent not-for-profit association)
A.12	Members of the Management Body	Jiang Bing – Chairman, Governance Committee Chen Weiran – President, Governance Committee Peng Zhonghua – Member, Governance Committee
A.13	Business Activity	The Association is a not-for-profit entity established to support the development, governance, and ecosystem growth of the zkPass Protocol and its associated digital assets. Its activities include funding protocol development, supporting community governance, ecosystem grants, and promoting the adoption of privacy-preserving verification technologies (zkTLS).
A.14	Parent Company Business Activity	N/A
A.15	Newly Established	True
A.16	Financial Condition for the past Three Years	Not applicable.
A.17	Financial Condition Since Registration	Since its registration in April 2024, the Association has been primarily funded through initial community and ecosystem grants dedicated to supporting zkPass Protocol development and operations. No debt or external financial liabilities have been incurred. Financial reporting will follow Swiss accounting standards, with the first audited financial statement expected for FY2024.
PART B - INFORMATION ABOUT THE ISSUER, IF DIFFERENT FROM THE OFFEROR OR PERSON SEEKING ADMISSION TO TRADING		

B.01	Issuer Different from the Person Seeking Admission to Trading	True
B.02	Name	IFCONNECT TECHNOLOGY LIMITED
B.03	Legal Form	Private Company Limited by Shares incorporated under the laws of the Republic of Seychelles.
B.04	Registered Address	306 Victoria House, Victoria, Mahe, Seychelles
B.05	Head Office	Not applicable.
B.06	Registration Date	17 April 2023
B.07	Legal Entity Identifier	237470
B.08	Another Identifier Required Pursuant to Applicable National Law	Not applicable – the Association is registered under Swiss civil law and is not required to maintain any additional identifier beyond its statutory registration in Zug.

B.09	Parent Company	Not applicable.
B.10	Members of the Management Body	Chen Weiran – Director Jiang Bing – Shareholder Peng Zhonghua – Shareholder
B.11	Business Activity	IFCONNECT TECHNOLOGY LIMITED is a private company limited by shares incorporated under the laws of the Republic of Seychelles. The company acts as the initial token issuer and administrative entity for the zkPass Protocol. Its activities include the technical minting and initial distribution of the ZKP tokens, execution of SAFT agreements with early purchasers, and temporary holding of proceeds from private and strategic sales. Following the Token Generation Event (TGE), the company transfers all governance and treasury functions to zkPass DAO (a Swiss association) and retains no control over the protocol or token smart contracts.
B.12	Parent Company Business Activity	Not applicable, see B.09 above.
PART C- INFORMATION ABOUT THE OPERATOR OF THE TRADING PLATFORM IN CASES WHERE IT DRAWS UP THE CRYPTO-ASSET WHITE PAPER AND INFORMATION ABOUT OTHER PERSONS DRAWING THE CRYPTO-ASSET WHITE PAPER PURSUANT TO ARTICLE 6(1), SECOND SUBPARAGRAPH, OF REGULATION (EU) 2023/1114		
C.01	Name	Not applicable
C.02	Legal Form	Not applicable
C.03	Registered Address	Not applicable

C.04	Head Office	Not applicable
C.05	Registration Date	Not applicable
C.06	Legal Entity Identifier of the Operator of the Trading Platform	Not applicable
C.07	Another Identifier Required Pursuant to Applicable National Law	Not applicable
C.08	Parent Company	Not applicable
C.09	Reason for Crypto-Asset White Paper Preparation	Not applicable
C.10	Members of the Management Body	Not applicable
C.11	Operator Business Activity	Not applicable
C.12	Parent Company Business Activity	Not applicable

C.13	Other Persons Drawing up the Crypto- Asset White Paper According to Article 6(1), Second Subparagraph, of Regulation (EU) 2023/1114	Not applicable
C.14	Reason for Drawing the White Paper by Persons Referred to in Article 6(1), Second Subparagraph, of Regulation (EU) 2023/1114	Not applicable
PART D – INFORMATION ABOUT THE CRYPTO-ASSET PROJECT		
D.01	Crypto-Asset Project Name	zkPass
D.02	Crypto-Assets Name	zkPass Token
D.03	Abbreviation	$ZKP
		The Protocol is not a distributed ledger itself but rather lives on multiple distributed ledger systems, such as

<table>
<tr><td>D.04</td><td>Crypto-Asset Project Description</td><td>The zkPass Protocol (“Protocol”) is a decentralized verification infrastructure that enables users to generate cryptographic proofs from private Web2 data without revealing the underlying information.
By leveraging the zkTLS standard, zkPass transforms existing HTTPS-based data—such as identity, financial records, learning progress, or reputation metrics—into portable zero-knowledge proofs that can be verified on -chain or within applications.
The Protocol functions as a foundational layer for the emerging Verifiable Internet, providing developers and organizations with privacy-preserving data attestations usable across DeFi, AI, GameFi, DePIN, and other Web3 domains.</td></tr>
<tr><td>D.05</td><td>Details of all Natural or Legal Persons Involved in the Implementation of the Crypto-Asset Project</td><td>List of Entities involved in development of the Ecosystem<table><tr><th>Full Name</th><th>Business Address</th><th>Function</th></tr><tr><td>zkPassDAO</td><td>Zug, Switzerland.</td><td>Governance</td></tr></table></td></tr>
<tr><td></td><td></td><td><table><tr><td>IFCONNECT TECHNOLOGY LIMITED</td><td>306 Victoria House, Victoria, Mahe, Seychelles</td><td>Issuer</td></tr><tr><td>Halborn Security</td><td>114 NW 25th Street, Miami, Florida, 33127, USA</td><td>Security (Audit)</td></tr><tr><td>Genesis Block</td><td>425 West 53rd Street, #405, New York, NY 10019, USA</td><td>Legal</td></tr></table></td></tr>
<tr><td>D.06</td><td>Utility Token Classification</td><td>True</td></tr>
</table>

D.07	Key Features of Goods/Services for Utility Token Projects	The Token provides access to the zkPass Protocol's core functionalities and ecosystem services, including: ● Proof Settlement: used to pay for verification and settlement of zero-knowledge proofs generated through zkTLS. ● Staking: required for verifiers and node operators to participate in proof validation and earn rewards. ● Governance: enables holders to participate in protocol governance, including decisions on technical parameters, treasury allocation, and ecosystem standards. ● Incentives: used to reward developers, users, and ecosystem partners contributing to proof generation, schema creation, and application integration. ● Access to Ecosystem Tools: including the zkPass SDK, DevHub, and Verifiable Application Acceleration Program (VAAP), allowing builders to integrate verifiable credentials and proofs.
D.08	Plans for the Token	The Token has undergone, or is expected to undergo, the following key events: ● Strategic and Private Sales conducted respectively during Q2 2024 and Q2 2025, raising funds to support ecosystem expansion and regulatory readiness. ● Launch on Ethereum Testnet (Sepolia) on 2025-05-20 (deployment transaction available on-chain). ● Launch on Arbitrum Testnet on 2025-07-15 (deployment transaction available on-chain). ● Full Protocol Launch on Ethereum Mainnet, planned for September 2025 (indicative and may be subject to change depending on strategic, regulatory, or market considerations). Following mainnet deployment, the Token will serve as the native settlement and governance asset within the zkPass Protocol, enabling staking, proof verification, and community-driven decision-making.
D.09	Resource Allocation	The funding secured through the private and strategic sales (see Section D.08 above) is devoted to the continued development and implementation of the zkPass Protocol. On the one hand, these resources have been allocated to build a multidisciplinary operations team of over 40 dedicated members, including specialists in zero-knowledge cryptography, blockchain engineering, Web3 community development, legal and compliance, marketing, and partnerships. On the other hand, the funds are primarily used to drive ecosystem growth by incentivizing user participation, supporting developers through grants, and fostering integration with existing DeFi, AI, and DePIN applications and partner blockchains.
D.10	Planned Use of Collected Funds or Crypto-Assets	Not applicable, because the Person Seeking Admission to Trading is seeking admission to trading and does not collect any funds in that context.

PART E – INFORMATION ABOUT THE OFFER TO THE PUBLIC OF CRYPTO-ASSETS OR THEIR ADMISSION TO TRADING		
E.01	Admission to trading	The Token is intended to be admitted to trading on one or more MiCA-registered trading venues within the European Union. The initial admission to trading will take place following the Token Generation Event (TGE), planned for December 2025, in coordination with regulated Crypto-Asset Service Providers (CASPs).
E.02	Reasons for the Admission to Trading	The admission to trading aims to provide secondary-market liquidity for the ZKP Token, facilitate transparent price discovery, and enable its use within the zkPass Protocol by a broad range of participants. Trading on regulated venues ensures that the Token operates under appropriate oversight, improving accessibility for ecosystem partners, verifiers, and community members.
E.03	Fundraising Target	Not applicable — no public fundraising is being conducted in connection with the admission to trading. All funds required for development and ecosystem expansion have already been raised through private and strategic sales completed in 2024–2025.
E.04	Minimum Subscription Goals	Not applicable. See explanation under E.03.
E.05	Maximum Subscription Goal	Not applicable. See explanation under E.03.
E.06	Oversubscription Acceptance	Not applicable. See explanation under E.03.
E.07	Oversubscription Allocation	Not applicable. See explanation under E.03.
E.08	Issue Price	Not applicable. See explanation under E.03.

E.09	Official Currency or Any other Crypto-Assets Determining the Issue Price	Not applicable. See explanation under E.03.
E.10	Subscription Fee	Not applicable. See explanation under E.03.
E.11	Offer Price Determination Method	Not applicable. See explanation under E.03.
E.12	Total Number of Traded Crypto-Asset	Potentially up to the whole supply of the Token, amounting to 1,000,000,000 (1 billion) Tokens, of which up to 18.17 % will be liquid upon admission to trading.
E.13	Targeted Holders	ALL, meaning both Retail (RETL) and Professional (PROF).
E.14	Holder Restrictions	Ethereum, the chain on which the Tokens are issued, is by design permissionless and decentralized. There are thus no restrictions at chain-level. The Trading Platforms in accordance with applicable laws and internal policies may similarly impose restrictions to those buying and selling the Token by placing trades on such Trading Platforms. Any checks performed to implement such restrictions, notably KYC checks, are not conducted by the Person Seeking Admission to Trading.
E.15	Reimbursement Notice	Not applicable. See explanation under E.03.
E.16	Refund Mechanism	Not applicable. See explanation under E.03.

E.17	Refund Timeline	Not applicable. See explanation under E.03.
E.18	Offer Phases	Not applicable. See explanation under E.03.
E.19	Early Purchase Discount	Not applicable. See explanation under E.03.
E.20	Time-Limited Offer	Not applicable. See explanation under E.03.
E.21	Subscription Period Beginning	Not applicable. See explanation under E.03.
E.22	Subscription Period End	Not applicable. See explanation under E.03.
E.23	Safeguarding Arrangements for Offered Funds/Crypto-Assets	Not applicable. See explanation under E.03.
E.24	Payment Methods for Crypto-Asset Purchase	The method of payment for the purchase and sale of the Token on the Trading Platforms will be determined unilaterally by the Trading Platforms or agreed upon mutually between the Person Seeking Admission to Trading and the relevant Trading Platforms. Such methods may include fiat (such as USD and EURO) and crypto assets (such as USDT or BTC).
E.25	Value Transfer Methods for	Not applicable. See explanation under E.03.

	Reimbursement	
E.26	Right of Withdrawal	Not applicable. See explanation under E.03.
E.27	Transfer of Purchased Crypto-Assets	The Tokens acquired as a result of trades shall be transferred to the compatible wallet or technical device as designated by the selected Trading Platforms. The Person Seeking Admission to Trading bears no responsibility for any transfers of the Token between market participants on the Trading Platforms.
E.28	Transfer Time Schedule	The transfer of the Tokens acquired as a result of trades conducted on the Trading Platforms may or not occur immediately, depending on the functioning of the selected Trading Platform. The Person Seeking Admission to Trading has no control over the timing of such transfers.
E.29	Purchaser's Technical Requirements	Token holder must comply with the technical requirements specific to the Trading Platforms on which the Token is admitted to trading, which may include the following: ● A compatible digital wallet or account on supported Trading Platform; ● Internet access; and ● A device (computer or mobile) to manage digital wallet/private key and/or account on exchange to carry out transactions.
E.30	Crypto-asset service provider (CASP) Name	Not applicable. See explanation under E.03.
E.31	CASP Identifier	Not applicable. See explanation under E.03.
E.32	Placement Form	Not applicable.

E.33	Trading Platforms Name	Admission to trading is being sought on Trading Platforms operating within the EU/EEA. As of the date of notification of the present White Paper, no listing agreement has been concluded; therefore, no specific Trading Platform can be identified at this stage. The most current list of available Trading Platforms will be at all times available on the Person Seeking Admission to Trading's website.
E.34	Trading Platforms Market Identifier Code (MIC)	Not available.
E.35	Trading Platforms Access	Trading Platforms are accessible via their respective website or applications for mobile device.
E.36	Involved Costs	The use of services offered by Trading Platforms may involve costs, including transaction fees, withdrawal fees, and other charges, as notified to users in advance. These costs are determined and set by the respective Trading Platforms and are not controlled, influenced, or governed by the Company. Consequently, any changes to initially announced fee structures or the introduction of new costs for the future are solely at the discretion of the Trading Platforms.
E.37	Offer Expenses	Not applicable. See explanation under E.03.
E:38	Conflicts of Interest	The Person Seeking Admission to Trading is not aware of any potential conflict of interest among its management body members or any other person within the Person Seeking Admission to Trading with respect to the admission to trading of the Token.
E.39	Applicable Law	Any dispute arising out of or in connection with the present White Paper, the Person Seeking Admission to Trading and the admission to trading shall be governed exclusively by the laws of Switzerland, without regard to conflict of law rules or principles, except to the extent that such disputes are governed by applicable law pursuant to the terms and conditions of the Trading Platform.
		Any dispute, controversy, or claim arising out of, or in relation to the present White Paper, the Person Seeking Admission to Trading, and the admission to trading shall be resolved exclusively by arbitration,

E.40	Competent Court	except to the extent that such disputes are subject to a dispute resolution mechanism set forth in the terms and conditions of the respective Trading Platform on which the Token has been admitted for trading. The arbitral proceedings shall be conducted in accordance with the Swiss Rules of International Arbitration of the Swiss Arbitration Centre in force on the date on which the Notice of Arbitration is submitted in accordance with those Rules. ● The number of arbitrators shall be three. ● The seat of the arbitration shall be Zürich, Switzerland. ● The arbitral proceedings shall be conducted in German. A respective arbitral award may only be challenged before the Swiss Supreme Court on the limited grounds as provided in Article 190 para. 2 Swiss Private International Law Act, i.e. (i) improper constitution of the arbitral tribunal; (ii) incorrect decision on jurisdiction; (iii) award beyond the claims submitted or failing to decide all claims submitted; (iv) violation of a party's right to be heard or of its right to equal treatment; and (v) incompatibility of the award with public policy.
PART F – INFORMATION ABOUT THE CRYPTO-ASSET		
F.01	Crypto-Asset Type	Utility Token
F.02	Crypto-Asset Functionalities	The Token serves four primary functions within the zkPass Protocol: 1. Settlement of Proofs — used as the medium of exchange for verifying and settling zero-knowledge proofs generated through the zkTLS framework. 2. Staking and Verification Collateral — verifiers and node operators must stake Tokens to participate in the verification network and earn rewards. 3. Governance — Token holders may propose and vote on protocol upgrades, treasury allocations, and changes to verification standards through zkPass DAO. All governance functions are exercised post-launch by zkPass DAO, following the transfer of control from the initial issuer, IFCONNECT TECHNOLOGY LIMITED. 4. Incentivization — used to reward developers, users, and partners who contribute to proof generation, schema creation, and ecosystem adoption. All functionalities are executed on-chain and are governed by smart contracts deployed on Ethereum and compatible Layer-2 networks.

F.03	Planned Application of Functionalities	The Token will be fully operational, with its core functionality available for use as of the Launch on Ethereum Mainnet, which will occur prior to any admission to trading.
A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset White Paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article		
F.04	Type of White Paper	OTHR
F.05	The Type of Submission	NEWT
F.06	Crypto-Asset Characteristics	The Token is a fungible digital asset initially issued by IFCONNECT TECHNOLOGY LIMITED (a private company limited by shares incorporated in the Republic of Seychelles) on the BSC/Base blockchain, compliant with the ERC-20 standard.The Issuer retains no control over the smart contract post-deployment. It has a fixed total supply of 1,000,000,000 (one billion) units and is designed to serve as the native utility and governance token of the zkPass Protocol. The governance of the Protocol is carried out by zkPass DAO (Swiss Association) as a separate non-profit entity. The Token is used for proof settlement, verifier staking, governance participation, and ecosystem incentives. No minting or burning beyond the fixed supply is planned. The Token is freely transferable, subject to applicable laws and vesting restrictions disclosed in this White Paper.
F.07	Commercial Name or Trading Name	$ZKP (zkPass Token)
F.08	Website of the Issuer	www.zkpass.org
F.09	Starting date of the Admission to Trading	No earlier than 2025-10-30

F.10	Publication Date	2025-10-09
F11	Any other Services Provided by the Issuer	The Issuer does not provide any ongoing services to token holders after the Token Generation Event. All governance and protocol operations are managed by zkPass DAO.
F.12	Identifier of Operator of the Trading Platform	Not applicable
4.F.13	Language or Languages of the White Paper	English
F.14	Digital Token Identifier Code used to uniquely Identify the Crypto-Asset or Each of the Several Crypto-Assets to Which the White Paper Relates, Where Available	Not applicable
F.15	Functionally Fungible Group Digital Token Identifier, Where Available	Not applicable

F.16	Voluntary Data Flag	False
F.17	Personal Data Flag	True
F.18	LEI Eligibility	Not applicable
F.19	Home Member State	Ireland pursuant to Article 3 (33) (c) of MiCA.
F.20	Host Member States	The admission to trading of the Token is passported in the following countries: Austria Belgium Bulgaria Croatia Cyprus Czechia Denmark Estonia Finland France Germany Greece Hungary Iceland Italy Ireland Latvia Liechtenstein Lithuania Luxembourg Netherlands Norway Poland Portugal Romania Sweden Slovakia Slovenia Spain
PART G – INFORMATION ON RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS		

G.01	Purchaser Rights and Obligations	The Token does not confer any rights or entitlements to its holders. The Issuer, IFCONNECT TECHNOLOGY LIMITED, disclaims all warranties, whether express or implied. Following the TGE, zkPass DAO, as a separate governance body, manages protocol operations without assuming issuer obligations.
G.02	Exercise of Rights and Obligations	Not applicable, see answer under G.1.
G.03	Conditions for Modifications of Rights and Obligations	Not applicable, see answer under G.1.
G.04	Future Public Offers	An airdrop campaign may be organized by zkPass DAO after the TGE as part of community distribution. The Issuer will not conduct or oversee any such distribution.
G.05	Issuer Retained Crypto-Assets	zkPass DAO is allocated 10% out of the initial total Token supply.
G.06	Utility Token Classification	True
G.07	Key Features of Goods/Services of Utility Tokens	The Token is a utility token that provides digital access to the Governance Functionality of the Protocol, as described in Section F.02. Such governance functionality is operated by zkPass DAO independently of the Issuer. The scope of the above-mentioned functionality may change based on decisions made through the Governance Functionality.

G.08	Utility Tokens Redemption	Not applicable
G.09	Non-Trading Request	True
G.10	Crypto-Assets Purchase or Sale Modalities	Not applicable. See explanation under E.3.
G.11	Crypto-Assets Transfer Restrictions	See field E.14 above.
G.12	Supply Adjustment Protocols	False
G.13	Supply Adjustment Mechanisms	Not applicable.
G.14	Token Value Protection Schemes	False
G.15	Token Value Protection Schemes Description	Not applicable
G.16	Compensation Schemes	False

G.18	Applicable Law	Any dispute arising out of or in connection with the present White Paper, the Person Seeking Admission to Trading, the Token and/or the Protocol shall be governed exclusively by the laws of Switzerland, without regard to conflict of law rules or principles, except to the extent that such disputes are governed by applicable law pursuant to the terms and conditions of the respective Trading Platform on which the Token has been admitted for trading. Disputes relating to the token governance and DAO activities are governed by Swiss law. Matters relating to the initial issuance and distribution of the Token are governed by the laws of the Republic of Seychelles.
G.19	Competent Court	Any dispute, controversy, or claim arising out of, or in relation to the present White Paper, the Person Seeking Admission to Trading, the Token and/or the Protocol shall be resolved exclusively by arbitration, except to the extent that such disputes are subject to a dispute resolution mechanism set forth in the terms and conditions of the respective Trading Platform on which the Token has been admitted for trading. The arbitral proceedings shall be conducted in accordance with the Swiss Rules of International Arbitration of the Swiss Arbitration Centre in force on the date on which the Notice of Arbitration is submitted in accordance with those Rules. ● The number of arbitrators shall be three. ● The seat of the arbitration shall be Zürich, Switzerland. ● The arbitral proceedings shall be conducted in German. A respective arbitral award may only be challenged before the Swiss Supreme Court on the limited grounds as provided in Article 190 para. 2 Swiss Private International Law Act, i.e. (i) improper constitution of the arbitral tribunal; (ii) incorrect decision on jurisdiction; (iii) award beyond the claims submitted or failing to decide all claims submitted; (iv) violation of a party's right to be heard or of its right to equal treatment; and (v) incompatibility of the award with public policy.
PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY		
H.01	Distributed Ledger Technology	The zkPass Protocol is not itself a blockchain or distributed ledger, but operates as an interoperability layer between Web2 HTTPS environments and Web3 smart contract systems. It utilizes Ethereum and Ethereum-compatible Layer 2 networks as its primary settlement and governance substrate. All stateful interactions — including staking, governance voting, and proof verification incentives — are recorded and finalized on Ethereum’s Proof-of-Stake (PoS) consensus layer. The zkPass off-chain components generate verifiable proofs that can be anchored or verified on-chain,

		without transmitting or storing any user data.
H.02	Protocols and Technical Standards	zkPass is based on a novel cryptographic composition of Three-Party Transport Layer Security (3P-TLS), Secure Multi-Party Computation (MPC), and Interactive Zero-Knowledge Proofs (IZK): ● TLS 1.3 / TLS 1.2 (RFC 8446 / RFC 5246) — Provides the underlying authenticated and encrypted HTTPS channel. zkPass extends TLS into a 3-party model, allowing proof extraction while maintaining standard compliance. ● X.509 Certificate Chains (RFC 5280) — Used to authenticate DataSources and validate the domain–certificate binding within proof contexts. ● ECDHE Key Exchange and AES-GCM/ChaCha20-Poly1305 Cipher Suites — Standard TLS mechanisms preserved within zkPass's modified handshake for session integrity. ● Oblivious Transfer (OT) and Garbled Circuits (GC) — Enable secure multi-party evaluation of TLS session states, preventing any participant from tampering or learning confidential values. ● HMAC (RFC 2104) and SHA-256 — Serve as verifiable message authentication mechanisms for TLS transcript integrity proofs. ● ICP-ZKP (Interactive Commit-and-Prove Zero-Knowledge Proof) — A memory-efficient, modular circuit proof system supporting large-scale computations across web data schemas. ● VOLE-based OT Extension (per Boyle et al., 2019) — Optimizes communication efficiency for large-scale OT instances. All zkPass cryptographic constructions strictly adhere to open standards and cryptographic best practices to ensure interoperability and formal verifiability
H.03	Technology Used	The zkPass Protocol combines secure client-side computation with decentralized verification infrastructure: ● 3P-TLS Session: The Prover (user) engages both the DataSource (HTTPS server) and the zkPass Node in a modified TLS handshake. This enables generation of a verifiable session transcript without exposing plaintext content. ● MPC Integrity Layer: During the handshake, the Prover and Node jointly hold shares of a session MAC key, ensuring neither can falsify or tamper with authenticated responses. The Verifier does not possess the encryption key and therefore cannot read user data. ● Interactive Zero-Knowledge Proof: Once data is retrieved, the Prover constructs an IZK proof demonstrating that the authenticated response satisfies specific assertions (e.g., "my Duolingo streak ≥ 50") without revealing the data itself. ● Modular Circuit Architecture: Large proofs are decomposed into reusable "gadget" circuits, reducing memory footprint and enabling browser-level performance.

		• On-Chain Verification and Settlement: Proof verification results, staking, and incentive distributions are recorded via smart contracts deployed on Ethereum. No personal data ever enters the blockchain. • Security Audit: The zkPass smart contracts and protocol libraries are independently audited by Halborn Security, ensuring conformance with industry security standards.
H.04	Consensus Mechanism	zkPass is a privacy-preserving verification infrastructure enabling individuals to transform private Web2 data (from HTTPS sources such as banks, exchanges, or educational platforms) into verifiable cryptographic proofs. Through its 3P-TLS + MPC + IZK framework, zkPass allows Web3 applications to consume these proofs securely, bridging Web2 trust data into decentralized systems. The protocol ensures end-to-end integrity, data authenticity, and zero-knowledge privacy — creating the foundational “proof layer” of the Verifiable Internet. The project is governed by zkPassDAO, a Swiss not-for-profit association established under Articles 60 et seq. of the Swiss Civil Code, which manages the protocol’s development, treasury, and token governance
H.05	Incentive Mechanisms and Applicable Fees	The zkPass network is sustained through a verifier–prover–staker incentive model designed to ensure network integrity and continuous verification availability. • Node Incentives: zkPass Verifier Nodes receive compensation in $ZKP tokens for successfully validating zero-knowledge proofs submitted by users. Rewards are dynamically adjusted based on the computational cost, transaction size, and staking weight of the node. • Staking and Delegation: Both node operators and community participants may stake $ZKP to secure the network. Staked tokens act as collateral for correct behavior; misbehavior or non-performance may result in partial slashing. Delegators earn a portion of verifier rewards. • Proof Fees: Users generating verifiable proofs pay a minimal service fee denominated in $ZKP or native gas tokens (e.g., ETH), covering the cost of computation and settlement. • DAO Treasury Allocation: A small percentage of protocol-level fees (currently 5%) is automatically routed to the zkPassDAO treasury to fund ecosystem grants, security maintenance, and open-source research.

		This economic framework aligns incentives across all participants while maintaining sustainable, low-cost proof verification.
H.06	Use of Distributed Ledger Technology	False. DLT is not operated by the person seeking admission to trading or a third-party acting on their behalf.
H.07	DLT Functionality Description	Not applicable.
H.08	Audit	True
H.09	Audit Outcome	An independent third-party audit of the zkPass technology was conducted by Halborn Security, focusing on the zkPass TransGate browser plugin and its interaction with the zkPass protocol. ● The audit scope included the verification of: ● Secure implementation of the 3P-TLS session handshake; ● Integrity of the browser-based zero-knowledge proof generation process; ● Data isolation between user sessions to prevent information leakage; and ● Code safety, permission handling, and update mechanisms within the TransGate extension.
PART J – INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS		
J-01	Adverse Impacts on Climate and Other Environment-	The zkPass Protocol has no material adverse impact on the environment or climate. The protocol operates primarily through off-chain cryptographic computation and lightweight smart-contract execution on Ethereum, a Proof-of-Stake (PoS) blockchain. Following Ethereum's transition to PoS, the network's annual energy consumption has been estimated at less than 0.01 % of that of Proof-of-Work blockchains.

	Related Adverse Impacts	zkPass itself does not maintain its own blockchain or mining network, and therefore does not directly contribute to high-energy consensus mechanisms. All user proofs are generated locally on consumer hardware using energy-efficient zero-knowledge circuits, with computational costs comparable to standard HTTPS encryption operations. The zkPassDAO continuously monitors sustainability metrics associated with its infrastructure providers and encourages node operators to host verification services on renewable-energy-powered cloud or datacenter environments. In summary, zkPass's operational footprint is negligible in terms of CO_2 emissions and aligned with the environmental objectives of Regulation (EU) 2023/1114 (MiCA).
S.01	Name	zkPass DAO
S.02	Relevant Legal Entity Identifier	Not applicable.
S.03	Name of the Crypto-Asset	$ZKP - zkPass Token
S.04	Consensus Mechanism	See H.04.
S.05	Incentive Mechanisms and Applicable Fees	See H.05.
S.06	Beginning of the Period to Which the Disclosure Relates	2025-01-01
S.07	End of the Period to which the	2025-12-31

	Disclosure Relates	
S.08	Energy Consumption	The estimated annual energy consumption associated with zkPass operations for the period 2025-01-01 to 2025-12-31 is approximately 36.8 kWh, well below the 500,000 kWh reporting threshold. This estimate covers the operation of validator nodes, the maintenance of Ethereum smart contracts, and the distributed verification infrastructure. All computations occur off-chain on standard consumer or cloud hardware, and on-chain transactions rely on Ethereum's Proof-of-Stake consensus, which has negligible energy impact relative to Proof-of-Work systems.
S.09	Energy Consumption Sources and Methodologies	Energy metrics are based on data from the Crypto Carbon Ratings Institute (CCRI) and publicly available analyses of Ethereum's post-Merge PoS consumption. All indicators represent modeled estimates using standardized assumptions: ● Average energy use per Ethereum transaction ≈ 0.0008 kWh (CCRI 2024). ● Extrapolated to an estimated 46,000 annual transactions related to zkPass operations. Further details are available via: https://carbon-ratings.com/dl/whitepaper-mica-methods-2024 and https://docs.mica.api.carbon-ratings.com.