Secure and Unified Identity Verification

【Overview of Secure and Unified Identity Verification】

I. Concept of Secure and Unified Identity Verification

Secure and unified identity Verification establishes unique digital identity credentials for taxpayers, payers, and tax officials, providing reliable identity authentication for all tax-related applications and building the cornerstone of identity trust in the tax cyberspace. It is not only the starting point for the digital transformation of tax collection and administration but also the solid foundation of the overall tax cybersecurity system.

Secure and unified identity Verification aims to break down information silos and build a unified national tax identity center, achieving "one-stop collection, mutual Verification across regions, one-time authentication, and nationwide accessibility." It breaks down the silos of identity information management across different vertical levels and horizontal internal and external information systems, achieving "mutual Verification and universal use" of user identities across systems. Relying on the "4A" system of identity management, identity authentication, access control, and risk auditing, it creates a unified national tax network identity that spans entities, regions, levels, and systems. It covers a unified user identity authentication source for legal persons, natural persons, and tax officials, providing a unique and trusted national network identity for all relevant entities involved in taxes, fees, and invoices. Simultaneously, it logs the entire identity verification process, enabling dynamic risk control and ensuring traceability and auditability of key behaviors.

II. Significance and Value of Secure and Unified Identity Verification

From the perspective of taxpayers, the core value of secure and unified identity identification lies in resolving all difficulties with one certificate and building a safe and convenient tax entrance. It completely solves the cumbersome and security risks of repeated registration and memorization of multiple sets of passwords on different platforms in the past, and liberates taxpayers from complex identity verification processes. After the completion of the National Unified Identity Center, the unit level covers for-profit legal persons, unincorporated organizations, non-profit legal persons (such as public institutions, social organizations) and special legal persons (such as party and government organs). At the individual level, it covers all related personnel such as tax payment, bill payment, invoices, tax incentives and expense deductions. Based on the "person-enterprise" relationship, the accounts and permissions of affiliated enterprises scattered in different provinces are collected as a "one-person" identity, supporting "one place login, national general office", and significantly improving the efficiency of taxpayers' tax handling.

From the perspective of the tax authorities, the core value of secure and unified identity Verification lies in strengthening the foundation of data governance and empowering the reform of tax collection and administration service models. A unified identity system is the key to connecting data scattered across various business systems, forming a complete "panoramic view of taxpayers," enabling big data analysis, intelligent pre-filling, and precise policy delivery. It constructs the first intelligent line

of defense for risk prevention and control, effectively identifying and blocking risks such as impersonation, theft, and false registration through multi-dimensional monitoring of login behavior, devices, and locations, curbing fraud before it occurs. Therefore, secure and unified identity verification is the underlying support and core engine for tax authorities to transform from decentralized management to centralized governance, from passive response to proactive service, and from experience-based decision-making to data-driven decision-making.

From the perspective of national (regional) tax governance, establishing a secure and unified identity verification system is the infrastructure for modernizing tax governance. It is not only a technological upgrade but also a strategic measure to break down departmental information barriers, restructure tax collection processes, and deepen international tax collection cooperation, thus possessing multiple significances. First, it breaks down information silos and reduces the cost of cross-system identity management. By assigning each taxpayer a unique digital identity, it enables automatic data linking across departments, resolving inconsistencies in data for the same taxpayer across different departments and systems. This significantly reduces manual comparison and repetitive data entry, lowering the investment and maintenance burden on both taxpayers and tax authorities in identity management. Second, it prevents identity theft and tax fraud, ensuring tax security. Utilizing technologies such as biometrics and digital certificates ensures that the registered entity is the real person and the operator is the actual person, effectively curbing illegal activities such as registering shell companies with false identities, issuing false invoices, and fraud. Third, it provides a unified basis for mutual Verification of identities for international tax cooperation. When implementing the Common Reporting Standard (CRS), a unified taxpayer identification number is a prerequisite for the automatic exchange of financial account information, ensuring clear attribution of profits for multinational corporations. In addressing digital economy taxation, a unified identity system also provides internationally identifiable identifiers for determining the "ultimate parent company" and "penetrating entity" of multinational corporations, avoiding double taxation or double non-taxation due to identity confusion.

【The Development History of Secure and Unified Identity Verification】

I. Decentralized Authentication and Initial Real-Name Registration Stage

Initially, tax authorities deployed identity verification systems independently across their various information systems, resulting in a "siloed" construction model. Commonly used technologies relied on physical media or static credentials such as U-keys, account passwords, and SMS verification codes. For example, Germany widely used electronic tax cards with card readers, while the US Internal Revenue Service initially used personal identification numbers and electronic certificates for tax filing.

The management logic at this stage focused on physical devices or static accounts, rather than the real identity of natural persons; that is, "recognizing devices" rather than "recognizing people." As long as one possessed a legal medium or had the password, it was considered successful, making it difficult to effectively confirm whether the operator was the taxpayer. At the same time, tax collection resources were dispersed across various system operations, forming a decentralized model. It was difficult to form a unified risk view; risks such as identity theft and false registration could only be addressed on a case-by-case basis, unable to be controlled on a large

scale.
This decentralized model brought some inconveniences: for instance, taxpayers had to repeatedly register and bind different U-keys on multiple platforms for different transactions, increasing tax processing costs and reducing efficiency. Furthermore, security risks were significant; lost U-keys could be misused, and weak passwords were vulnerable to credential stuffing attacks. Later, to address high-risk scenarios such as identity theft and fraudulent registration, some systems introduced real-name verification measures, such as uploading ID documents, manual comparison, or relying on third-party authentication services to complete "identity verification." However, the above measures are limited to specific businesses or regions, creating new "data silos"—systems cannot share real-name information, and cross-system and cross-regional identity Verification cannot be achieved. Overall, the authentication system at this stage is characterized by "each operating independently and not interconnected," which not only increases the burden on taxpayers but also creates obstacles for subsequent unified identity governance.

II. Unified Portal and Online Real-Name Registration Stage
In order to further improve the user experience and security protection level of e-government services, countries have successively launched the construction of unified e-government or industry portals to promote the identity verification system from decentralized to centralized. The core of identity verification at this stage is to integrate a multi-factor verification mechanism, establish basic audit logs, and connect with authoritative population information databases in real time to achieve online real-name verification with "consistent identity of people". Users only need to authenticate once to access all business systems in the portal, significantly improving security and convenience. In this process, countries generally attach importance to privacy protection, follow the principle of "minimum necessary" to collect user information, and reduce the risk of privacy leakage through measures such as user authorization and data encryption.
The limitations of this stage are: First, online authentication and offline windows are not yet fully integrated, and some businesses still require offline verification, affecting the closed-loop management of the entire process; second, the cross-regional identity mutual Verification mechanism is not yet perfect, and there is a lack of unified mutual trust standards between different administrative regions or countries. Users often need to verify repeatedly when handling business in different places, or face the problem of being unable to verify. These bottlenecks directly promoted the construction of the next stage of the unified identity system.

III. Unified Identity Verification and Intelligent Risk Control Stage
With the continuous deepening of the demand for data sharing and business collaboration, countries and regions are shifting towards the construction of national or regional unified identity verification centers to promote the centralized and unified management of the identity information of natural persons and legal persons. The core feature of this stage is that identity verification fully supports roaming authentication across administrative regions and business systems, realizing a fundamental shift from "recognizing devices" to "recognizing people". Based on this, multimodal biometrics such as facial Verification, fingerprints, and iris scans are integrated, and behavioral analysis technology is introduced to build an intelligent risk engine, enabling real-time risk monitoring and automatic response.
Identity verification at this stage truly achieves "one-stop collection, mutual

Verification across regions, one-time authentication, and nationwide access," and can implement mandatory multi-factor authentication for highly sensitive operations based on risk behavior profiles. Taking the EU as an example, the cross-member state electronic identity mutual Verification framework established according to the eIDAS regulation allows national eIDs from countries such as Germany, Spain, and Italy to be used in the tax and social security systems of other member states, effectively supporting enterprises to "register in one place and handle all matters across Europe." For example,Singapore has also been making steady progress in extending the use of its nationwide digital identity system, SingPass from government transactions to a growing range of private sector uses. It is currently piloting ways to facilitate seamless cross-border verification and trusted compliance across business sectors. in 2021, the State Taxation Administration of China established a trusted identity system for the tax network, enabling the collection of information on related enterprises nationwide through a "one-person" system, effectively supporting "nationwide interoperability."

Overall, the construction of a unified identity center breaks down regional and system barriers under the traditional authentication system. At the same time, while placing greater emphasis on privacy protection, it relies on user behavior logs and big data technology to achieve dynamic risk prevention and control, laying a solid foundation for building a secure, convenient, and mutually trusting digital governance environment.

【Guidelines for the Development Stages of Secure and Unified Identity Verification】

Stage 1: Basic Unification and Online Real-Name Verification (Applicable to countries/regions in the early stages of digital tax administration)

The core task of this stage is to establish a unified online identity verification entry point, achieve full coverage of online real-name verification for key businesses, and solve the basic online verification problem of proving "I am me".

(I) Objectives and Platform Construction. The primary objective is to build or upgrade a unified online tax bureau portal as the sole official entry point for all online services. This portal integrates multiple identity authentication methods, including account passwords, mobile verification codes, and digital certificates. Mandatory online real-name verification is required for individual users handling core business such as invoices, declarations, and inquiries, with authoritative databases (such as the public security population database).

(II) Implementation Path. Online real-name verification will be mandatory in high-risk access stages such as new taxpayer registration, invoice type verification, and general taxpayer registration. Simultaneously, dispersed user data from various internal systems will be integrated to establish a preliminary unified taxpayer identity information database, including basic identity identifiers (such as unified social credit code and ID card number), and real-name information of key personnel such as legal representatives and financial officers.

(III) Supporting Systems and Capacity Building. This includes: formulating relevant management measures for identity authentication, clarifying the legal effect of online real-name authentication, the rights and responsibilities of all parties, and information

security standards; conducting large-scale taxpayer publicity and operational training; reserving alternative channels such as offline window authentication and telephone voice assistance for the elderly and those with low digital literacy; establishing the principle of "minimum collection," clarifying that information collection is limited to identity verification purposes.
(IV) Expected Results. Through this phase of construction, the online real-name processing rate of core businesses will be significantly improved, online anonymous operations will be basically eliminated, and fraudulent registrations will be curbed at the source. A unified identity portal provides taxpayers with a clear tax filing path and accumulates the most basic credible identity data assets for tax authorities.

Phase Two: Intelligent Upgrade and Online-Offline Integration (Applicable to countries/regions with moderate digitalization levels)
The core task of this phase is to promote identity authentication from "unified" to "intelligent" and from "online" to "online-offline integration" through technological empowerment, and to build a dynamic and multi-dimensional trust assessment system.
(I) Goals and Capability Enhancement. The goal is to reduce the authentication burden on compliant taxpayers while accurately identifying and intercepting high-risk identity misuse. Key performance indicators include taxpayer authentication success rate, average authentication time, and high-risk interception accuracy rate.
(II) Implementation Path. Build an intelligent risk engine to analyze login time, location, device, frequency, and other behaviors in real time, triggering secondary verification or direct interception for abnormal behaviors. Achieve mutual Verification of online and offline identities. After taxpayers complete identity verification at the tax service hall by facial Verification or QR code scanning, the authentication process can be simplified when handling related business online.
(III) Supporting Systems and Capacity Building. This includes: revising relevant regulations to clarify the legal boundaries and privacy protection requirements for the collection and use of biometric information such as facial Verification; establishing a regular audit and evaluation mechanism for authentication algorithm models; providing alternatives to non-biometric features (such as dynamic tokens and voice verification), regularly deleting original biometric images, and storing only feature codes; and retaining offline window services for real-name verification for the elderly and those with low digital literacy.
(IV) Expected Results. Through intelligent transformation, a "seamless" or "second-level" authentication experience will be provided for high-credit taxpayers, and a dynamic firewall will be built for high-risk behaviors. The integration of online and offline identities marks the formal formation of a taxpayer-centric continuous service experience.

Phase Three: Ecosystem Mutual Verification and Seamless Credit Access (Applicable to Digitally Mature Countries/Regions)
The task of this phase is to integrate tax identities into a broader national digital trust ecosystem, achieving "seamless access" based on credit and context, and supporting collaborative governance across society.
(I) Goals and Ecosystem Building. The ultimate goal is to break down organizational boundaries, enabling verified tax digital identities or identity credentials to be securely and smoothly mutually recognized and used between government departments and even with trusted commercial platforms.

(II) Implementation Path. Adopt international or national digital identity interoperability standards to ensure that tax identity credentials can be verified and accepted by other departmental systems. Securely output standardized identity verification capabilities to government platforms, banks, core enterprises in the industrial chain, etc., in the form of APIs, etc., and support them to efficiently verify the tax qualifications of enterprises in scenarios such as credit and business cooperation while ensuring privacy.
(III) Supporting Systems and Capacity Building. This includes: promoting the introduction of cross-departmental digital identity mutual Verification and data sharing agreements, establishing joint supervision and dispute resolution mechanisms; regulators should clarify the "minimum necessary" data sharing principle, requiring individual user authorization for each cross-domain call; establishing a distributed identity mechanism, allowing users to selectively disclose attributes without exposing their real identity; retaining a "simplified authentication channel" in ecosystem mutual Verification, allowing elderly people and those with low digital literacy to authorize relatives to assist in authentication or use voice commands.
(IV) Expected Results. Taxpayers can access various government services using a single trusted identity, achieving "one-time authentication, access across the entire network." Under controllable risks, tax authorities have minimized the interference of identity verification for compliant taxpayers, truly achieving "silent compliance." The identity system has become the digital trust cornerstone for activating data elements and optimizing the business environment.
Appendix: Comparison Table of Different Identity Authentication Technologies

Authentication Method	Applicable Scenarios	Security Level	Cost	Applicable Stage
Account Password	Low-Risk Inquiry	Low	Extremely Low	Stage One
SMS / Email Verification Code	Medium-Risk Business	Medium	Low	Stage One & Two
Digital Certificate / UKEY	High-Risk Declaration	High	Medium	Stage One & Two
Facial Verification	High-frequency business	Medium-high	Medium	Phase Two & Three
Multi-factor combination	Core sensitive operation	Extremely high	Relatively high	Phase Two & Three
Behavioral biometrics	Continuous trust assessment	Extremely high	High	Phase Three

【Typical Case of Secure and Unified Identity Verification】

[China] Trusted Identity System for Tax Network
The tax network trusted identity system has built a "4A" system of identity management (Account), identity authentication (Authentication), access control (Authorization), and risk auditing (Audit). It has connected authoritative identity authentication sources from the Ministry of Public Security, the Immigration Bureau, the Market Supervision Bureau, and government service platforms, forming the first unified user identity authentication source in the country covering legal persons,

natural persons, and tax persons. It provides a unique and trustworthy online identity for various tax, fee, and invoice-related entities nationwide. It is the starting point for the digital transformation of tax collection and management and the cornerstone of the construction of a cybersecurity system.

[China] Electronic Invoice Service Platform

The electronic invoice service platform covers the entire lifecycle management of invoices, including issuance, delivery, verification, deduction, accounting, and archiving. It replaces the tax control equipment in the original invoice business with a trusted identity system for the tax network, providing unified real-name authentication services for both the invoice issuer and the invoice recipient, and performing dynamic identity verification in the invoice issuance and deduction selection processes. By employing identity authentication technologies such as facial Verification and SMS verification codes, the system rigorously verifies the ownership relationship between operators and their affiliated companies, ensuring consistency between individuals and enterprises and matching business permissions. This eliminates risks such as fraudulent issuance and impersonation at the source, guaranteeing the legal validity and data security of every electronic invoice. It makes all invoice-related activities traceable and auditable, truly achieving precise, end-to-end supervision and service based on trusted identities in the context of shifting from "tax control through invoices" to "tax administration through data."

[UAE] UAE Pass Digital Identity Authentication System

The Federal Tax Authority of the United Arab Emirates is vigorously promoting UAE Pass and regards it as the preferred national solution for digital identity authentication. UAE Pass provides a secure and government-supported digital identity framework that supports multi-factor authentication, including digital signatures, SMS or email verification codes, and username plus password, to ensure that identity verification complies with national digital government standards.

Meanwhile, UAE Pass has integrated with systems such as the Federal Identity, Citizenship, Customs and Port Security Authority to verify UAE ID card information and automatically retrieve authenticated identity data. Cross-validation with the national authoritative identity database further enhances the reliability and integrity of the identity verification process.

In addition, all digital communications and API interfaces operate through encrypted channels and use controlled access credentials, complying with relevant national cybersecurity and data protection standards.

[Hungary] Central Authentication Agent System

The Hungarian tax authorities use a central authentication agent system covering the entire Hungarian public administration sector for identity authentication. This service is responsible for authenticating users' identities; after successful authentication, users can access the tax system to handle tax-related matters.

The central authentication agent system provides two authentication methods: one is to install and activate a digital citizen application on a smart device as an identity authentication method. The other is a two-factor authentication method through a portal website + service. Taxpayers first enter their username and password to complete the first factor authentication, and then use a one-time token generated by an application pre-registered on theugyfelkapu.gov.huwebsite for authentication. The former applies only to Hungarian citizens, while the latter also applies to foreign

citizens.
Currently, the Hungarian tax authorities are introducing the EU's Electronic Identity and Trust Service (eIDAS) authentication method, which will enable citizens of other EU member states to use their own national electronic identity authentication services for identity verification.

[Saudi Arabia] Nafas Unified Digital Identity System
The Saudi tax authorities use Nafas for identity verification, the official unified digital identity system of the Kingdom of Saudi Arabia. It utilizes national identity card or residence permit data and securely verifies user identities based on Abu Shirley's authentication. Through multi-factor authentication and real-time verification, Nafas ensures that only legitimate individuals verified by the government can access tax services. This prevents fraud or unauthorized filings, thereby strengthening overall tax compliance.
Nafas protects its identity authentication system through strict information security controls, including protecting the confidentiality and integrity of taxpayer data and conducting regular audits and security updates to eliminate vulnerabilities. Nafas ensures that only authorized users can approve or submit sensitive transactions by enforcing multi-factor authentication.

[Mongolia] Electronic Tax System
The Mongolian tax authorities have built an identity verification function in the "Electronic Tax System," using a two-factor authentication method of login credentials (unique registration number and password) + email or mobile phone verification code. During this process, the registration number is cross-checked with the information of the authorized registration authority to verify its consistency with the registration information of the mobile phone number holder. The infrastructure (servers and networks) of the identity verification function follows international standards and is equipped with necessary network security equipment, systems, and technologies to prevent network attacks.
Since 2022, the Mongolian tax authorities have implemented the ISO/IEC 27001 Information Security Management System (ISMS) standard in their operations. Within this framework, they ensure that taxpayers' personal and corporate confidential data is securely stored, kept confidential, and protected, and is appropriately used, processed, and transmitted within the clearly defined rights, responsibilities, and requirements, in accordance with applicable laws, regulations, and procedures.

[Future Development Prospects of Secure and Unified Identity Verification]

Looking to the future, the tax authorities' secure and unified identity Verification system will evolve towards greater intelligence, ubiquity, and integration, driving a paradigm shift in tax governance at a higher level.

I. From "Identity Verification" to "Behavioral Credit Intelligent Agent"
The system can deeply integrate artificial intelligence and big data analysis. Future identity Verification will not only "prove who you are," but will also dynamically assess the "credit characteristics" and "risk genes" of taxpayers based on continuous behavioral data. The system can predict potential violations, shifting from "post-event accountability" to "precise pre-event guidance and intelligent in-event intervention."

II. A Key Node for Digital Citizenship and the Circulation of Data Elements

Tax digital identities are mutually recognized and interoperable with other digital identities of individuals and enterprises (such as government, medical, and financial identities), becoming an important component in building a national digital citizen identity system. Simultaneously, under the protection of legal authorization and secure privacy computing technologies, tax-related data based on trusted identities on the tax network will become high-value data elements that can circulate securely within a specific scope, empowering broader socio-economic fields such as inclusive finance and commercial credit.

III. A Penetrating and Dynamic Identification Mechanism to Address New Business Models

To address the challenges of ambiguous taxpayers and ineffective territorial jurisdiction in the platform economy and new individual economy, the system needs to develop dynamic identity Verification and association capabilities that can penetrate complex transaction chains and are based on substantive economic elements (such as capital flows, contract flows, and business flows). For example, by leveraging technologies such as blockchain-based evidence storage and privacy computing, identity verification can be cross-verified in real time with fund flows, contract flows, and business flows. This establishes taxpayer identification rules based on economic substance, providing technical support for the division of tax jurisdiction in the platform economy. This is the technical prerequisite for establishing tax jurisdiction rules under new business models and ensuring a fair tax base.

In short, a secure and unified identity verification system has transcended the realm of a mere technical tool; it is evolving into a core hub connecting taxpayers and tax authorities, breaking down data silos, and reshaping tax governance relationships. Its continued evolution will provide a solid foundation for improving modern tax governance capabilities.