identity_layer.md

📘 Назначение

Документ описывает идентификационную архитектуру участников системы AIUZ/UBITIQUE. Входит в уровень L3, поддерживает DAO, семантическую устойчивость и защиту от анонимных атак.

🧾 Подход к идентификации

- Используется модель **SSI (Self-Sovereign Identity)**
- Все участники управляют своими ID через криптографические ключи
- Данные размещаются вне блокчейна — ссылки или хеши (privacy-by-design)

🪛 Формат идентификатора

- Стандарт: `did:web`, `did:key` или `did:aiuz`
- Пример: `did:aiuz:stakeholder:0x8a3f...`
- Каждая роль в DAO (user/operator/auditor) имеет свой DID

🔐 Аутентификация и авторизация

Механизм	Назначение
Cryptographic Signature	Подтверждение участия в голосовании, внесении изменений
Token-Gated Access	Определение прав на доступ к API / ресурсам
Audit Log	Привязка действий к DID с проверкой времени

🧰 Связь с DAO и Stake Registry

- Каждое DID отображается в `stake_registry.json`
- Включает:
- роль,
- stake баланс (UTIL, GOV, REP),
- список публичных действий,
- репутационный индекс

🛠️Верификация участников

- Автоматическая: по stake + токенам + DID-чек
- Ручная: через аудитора или мультиголосование
- Метка "verified" даёт право на предложение/вето

📎Связь с другими слоями

Слой	Элемент
L0	Trace, Stakeholder (как агент)
L1	Протоколы валидации данных
L3	DAO: голосование, репутация
L4	Привязка логики пользователя к сессиям

📅Версия и статус

- Версия: id.v0.1 (2025-07-07)
- Совместим с W3C DID-Core, AIUZ Governance Layer v0.1
- Готов к расширению на KYC/AML сценарии и биоаутентификацию