Patent-Pending Dynamic Security Architecture for Zero-Risk Authentication Across IoT, Robotics, and Digital Platforms

A next-generation security architecture that unifies **UDAS (Universal Dynamic Authentication System)** and **DSS (Dynamic Security System)** into a single, mathematically unexploitable authentication model designed for IoT devices, robotics, industrial systems, cloud platforms, and large-scale digital services.

This architecture eliminates passwords, IC cards, certificates, fixed secrets, reusable tokens, and all forms of static authentication.

Instead, it generates **purpose-specific, one-time, self-destroying authentication keys** that cannot be reused, cloned, stolen, phished, extracted, or replayed.

🔐 **Key Capabilities**

- **Zero-Reuse, Zero-Risk Authentication** (keys destroy themselves automatically)
- **No Stored Secrets** (nothing exists for attackers to steal)
- **Replay Attack–Proof / Impersonation-Proof / Cloning-Proof**
- **Zero-Decompression Verification** (fast, lightweight, hardware-independent)
- **Real-time Key Generation & Destruction**
- Works on **MCUs → Embedded Devices → Robots → Industrial Machines → Cloud Platforms**

📄 **Patent Status**

Patent-Pending (JP Application No. **2024-172823**)

Includes rights for **licensing, joint development, or full acquisition**.

📘 **Whitepaper (DOI – Zenodo)**

https://doi.org/10.5281/zenodo.17845912

💻 **Prototype & Technical Details (GitHub Files Below)**

This repository contains sample code, schema designs, and implementation notes for early adopters evaluating the architecture.

📬 **Contact**

info@xinse.jp

Open to discussions on **licensing**, **collaboration**, or **acquisition** for

organizations developing next-generation security solutions.