Dynamic Non-Reusable Authentication Artifact (DNRA) Model for Securing Biometric Identity Systems Eliminating Biometric Vulnerabilities Using UDAS/DSS Zero-Risk Authentication Architecture A New Paradigm of Secret-Free, Non-Replayable Identity Verification

Author:
Yoshikazu Nakamura
Independent Researcher / Inventor
Japan
Email: info@xinse.jp
LinkedIn: https://www.linkedin.com/in/y-nakamura-ai/
GitHub: https://github.com/xinse-cyse

Patent Status:
This research is supported by the patent-pending technology:
Japan Patent Application JP 2024-172823
"Dynamic Security Generation AI System" (pending)
Keywords:
Biometric security, dynamic authentication, zero-risk authentication, UDAS/DSS, DNRA, cryptography, identity verification, non-replayable authentication, secret-free authentication model.

Abstract

Biometric authentication systems provide convenience but suffer from structural vulnerabilities that cannot be fixed by traditional cryptographic methods.

Biometric identifiers are static, non-replaceable, and easily subject to replay, cloning, spoofing, and irreversible compromise. Existing authentication models—including passwords, tokens, certificates, and FIDO-based public-key authentication—ultimately rely on reusable secrets, making them inherently vulnerable to theft.

This paper introduces **UDAS/DSS (Universal Dynamic Authentication**

System / Dynamic Security System), a new authentication architecture that eliminates stored secrets entirely and generates **Dynamic Non-Reusable Authentication Artifacts (DNRA)**. DNRA are ephemeral, non-reconstructible, non-replayable constructs that enable identity verification without persistent credentials, key material, or biometric templates.

We show how UDAS/DSS integrates with biometric authentication to neutralize all structural biometric weaknesses. The biometric match remains local, while identity verification is achieved through DNRA, ensuring that biometric data cannot be replayed, exported, cloned, or exploited—even under full device compromise. We provide formal security analysis, architectural descriptions, use cases, and comparisons with conventional technologies including FIDO2, PKI, and zero-knowledge models.

UDAS/DSS represents a new class of authentication—**the first paradigm capable of achieving zero-risk authentication in theory and practice**—and establishes a foundation for future identity systems across smartphones, cloud environments, IoT, robotics, industrial systems, automotive security, and critical infrastructure.

Table of Contents

(UDAS/DSS + Biometric Security Integration)

1. Introduction

1.1 Background and Motivation

Modern authentication systems fundamentally rely on one persistent assumption:

a secret must exist, must be stored, and must remain unexposed.

Passwords, tokens, certificates, and even biometrics all adhere to this

paradigm.
However, decades of security incidents demonstrate that any secret that exists
will eventually leak, be duplicated, or be manipulated.
This structural fragility represents the foundational weakness of digital security.
At the same time, biometric authentication has gained widespread adoption due to
its usability and convenience. Nevertheless, its security properties have
remained largely unchanged—the biometric template is static, and once leaked,
cannot ever be replaced. As a result, biometrics solve the usability problem
but not the security problem.
To address this global and persistent structural failure,
we introduce **UDAS/DSS (Universal Dynamic Authentication System / Dynamic Security System)**,
a novel authentication paradigm that eliminates stored secrets entirely and
generates authentication artifacts that are **non-reusable, non-reconstructible, and ephemeral**. This paper further examines the integration of UDAS/DSS with
biometric authentication to eliminate the inherent weaknesses of biometric systems.

1.2 Structural Weaknesses of Existing Authentication Systems

The dominant authentication systems today share several fatal properties:

- Reliance on long-term secrets
- Vulnerability to replay, cloning, and impersonation
- Attack surfaces in both client and server
- Dependence on secure storage elements
- Inability to prevent credential leakage

These weaknesses are not implementation flaws—they are **logical consequences**
of secret-based authentication.

1.3 Limitations of Biometric Authentication

While biometrics remove the need for passwords, they introduce even more dangerous risks:

- Templates cannot be replaced once compromised
- Biometric decisions can be intercepted or replayed
- Spoofing attacks remain possible
- Device compromise results in total identity compromise

Because biometrics are inherently static, they cannot achieve cryptographic properties such as forward secrecy or non-replay.

Thus, biometrics require a complementary system that neutralizes their structural weaknesses.

1.4 Contribution of This Paper

This paper provides the following key contributions:

1. **We formalize UDAS/DSS as a new class of authentication architecture** independent of passwords, tokens, biometrics, or stored secrets.
2. **We define the Dynamic Non-Reusable Authentication Artifact (DNRA)** as a mathematical construct enabling zero-risk authentication.
3. **We demonstrate how UDAS/DSS eliminates the core vulnerabilities of biometric authentication** without modifying biometric algorithms.
4. **We provide security analysis, system architecture, and comparative evaluation**
   demonstrating that UDAS/DSS represents a fundamentally distinct paradigm
   from existing cryptographic or biometric models.

1.5 Structure of This Paper

Section 2 reviews related work.

Section 3 describes the threat model.

Section 4 introduces the UDAS/DSS architecture.

Section 5 explains its integration with biometrics.

Section 6 presents formal security analysis.

Section 7 describes system architecture.
Section 8 discusses applications.
Sections 9–12 provide analysis, comparison, and conclusions.

2. Related Work

2.1 Password- and Token-Based Authentication

Traditional authentication requires storing reusable secrets such as passwords,
hashes, API keys, or private keys. Even when encryption or secure hardware is
used, the authentication ultimately depends on information that must remain confidential. Numerous breaches demonstrate that storing secrets is a
long-term systemic vulnerability.

2.2 Biometric Authentication Models

Biometric systems rely on physiological or behavioral characteristics that are assumed to be difficult to duplicate. However, they are vulnerable to:

- Spoofing
- Template theft
- Replay attacks
- Device compromise

Most critically, biometric data cannot be revoked or replaced, making compromise irreversible.

2.3 Cryptographic Approaches to Dynamic Authentication

Zero-knowledge proofs and challenge–response protocols attempt to reduce exposure of secrets, but all still require:

- A secret that persists somewhere
- A computational basis that is ultimately reproducible
- Vulnerability to replay or man-in-the-middle attacks

None of these methods eliminate the notion of a long-term shared secret.

2.4 Zero-Trust Architectures and Current Gaps

Zero-trust frameworks improve network-level assurance but do not solve the authentication problem itself. They still depend on passwords, certificates, or biometrics as the root of trust.
Thus, zero-trust infrastructures cannot achieve true zero-risk authentication.

2.5 What Prior Work Fails to Solve

Across all existing approaches, the same structural flaw persists:
If a secret exists, it can be stolen.
If it can be reused, it can be replayed.
If it can be replayed, it can be impersonated.
No prior work addresses the fundamental requirement for a system that **uses no persistent secrets at all**.
UDAS/DSS is the first architecture to satisfy this requirement.

3. Threat Model and Security Assumptions

3.1 Adversary Capabilities

We assume an adversary with strong capabilities:

- Full network interception
- Access to client-side memory
- Ability to compromise biometric sensors
- Ability to steal cryptographic keys from existing systems
- Full replay capability

UDAS/DSS is designed such that none of these capabilities result in successful impersonation.

3.2 Attack Surfaces in Conventional Systems

Traditional systems expose:

- Stored key material
- Transmittable authentication data
- Biometric templates
- Static signatures
- Tokens and certificates

All of these represent reusable objects and therefore security liabilities.

3.3 Analysis of Biometric-Specific Threats

Biometrics add the following risks:

- Template extraction
- Sensor spoofing
- Irreversibility of identity compromise
- Replay of "biometric match = true" signals

These vulnerabilities highlight the necessity of a non-reusable authentication mechanism.

3.4 Requirements for a Zero-Risk Authentication System

A system must:

1. Use no stored secrets
2. Generate no reusable outputs
3. Produce authentication artifacts that cannot be reconstructed
4. Resist replay under any circumstance
5. Allow biometric integration without exposing biometric data

Only UDAS/DSS satisfies all these requirements simultaneously.

4. Overview of the UDAS/DSS Architecture

4.1 Fundamental Design Principles

UDAS/DSS is founded on a new principle in authentication theory:

authentication should not depend on any persistent secret—either stored or derivable—on any device or server.

Unlike cryptographic systems that rely on long-term keys, UDAS/DSS generates

authentication artifacts that are:

- **Ephemeral** (exist only during a single session)
- **Non-reproducible** (cannot be regenerated from any prior or future state)
- **Non-replayable** (valid only within a defined temporal or contextual bound)
- **Stateless** (servers store no secrets related to user identity)

The absence of persistent secrets eliminates the surface on which most attacks occur.

4.2 Dynamic Non-Reusable Authentication Artifact (DNRA)

At the core of UDAS/DSS is the **Dynamic Non-Reusable Authentication Artifact (DNRA)**,
a data construct generated at authentication time that serves as a one-time proof of identity.
A DNRA satisfies the following properties:

1. **Non-reusability**: Once used, it is computationally useless.
2. **Non-reconstructibility**: No mathematical reverse path exists.
3. **Contextual binding**: Includes session-specific entropy, device state, and contextual factors.
4. **Zero persistence**: No component of DNRA is stored before or after authentication.

Formally, if S is a session, C the context, and E entropy,
then the DNRA is:
DNRA = f(S, C, E)
Where f is non-invertible, non-repeatable, and not bounded to any secret.

4.3 Elimination of Stored Secrets

In contrast to key-based authentication systems, UDAS/DSS eliminates:

- Passwords
- Secret keys
- Biometric templates
- Tokens
- Certificates
- Cryptographic material that persists between sessions

This approach removes the root cause of credential theft and impersonation:
the existence of a reusable object that proves identity.

4.4 Ephemeral Session Binding Mechanism

The authentication process is strictly bounded by:

- **Time intervals**
- **Session identifiers**
- **Device and system state**
- **Non-deterministic entropy sources**

Because these components cannot be reproduced exactly, even by the same device,
a DNRA cannot be recalculated once lost.
This property ensures **replay attacks are mathematically impossible**,
not merely prevented by protocol checks.

4.5 Formal Properties of Irreversibility and Non-Replay

The DNRA function f is designed such that:

1. Irreversibility

There is no mapping from DNRA back to (S, C, E).
The destruction of entropy components ensures non-invertibility.

2. Non-replay

$DNRA(S_1) \neq DNRA(S_2)$
for any $S_1 \neq S_2$, even if all other inputs appear identical.

3. Forward Unlinkability

DNRA artifacts cannot be correlated across sessions.

4. Stateless Verifiability

The server validates DNRA without storing secrets.
This enables fully secure authentication **without key management**,
a capability absent in all prior authentication technologies.

5. Integration With Biometric Authentication

5.1 Motivation for Integration

Biometric authentication is widely deployed but carries unavoidable weaknesses:

- Templates are static
- Leakage is permanent
- Replay of “success signals” is trivial
- Device compromise exposes the entire identity

UDAS/DSS provides a path to secure biometrics by eliminating the ability to reuse
biometric outputs.

5.2 Local Biometric Validation as a Trigger Mechanism

In the integrated architecture:

1. The user presents biometric data (face, fingerprint, etc.)
2. The **match decision remains local** and is never transmitted
3. Upon match, the system **generates DNRA** for authentication

Biometric data never leaves the device.
Only a dynamic, one-time authentication artifact is produced.
This removes:

- Biometric template exposure
- Biometric replay attacks
- Intercepted success-state duplication

5.3 Generation of DNRA After Biometric Match

The biometric match acts as a **gatekeeper** for DNRA generation.
If B is the biometric match event,
the DNRA is defined only if:
B = true
DNRA = f(S, C, E, B)
But because B has no externally accessible representation,
an attacker cannot:

- Reproduce B
- Replay B
- Force DNRA creation

This creates the world's first biometric system where **the biometric event is unspillable**.

5.4 Security Implications

5.4.1 Removing Biometric Reusability

Biometric signals are static and therefore dangerously reusable.

UDAS/DSS breaks this link:
the output changes at every authentication.

5.4.2 Neutralizing Spoofing and Replay

Even if an attacker perfectly mimics a fingerprint or face,
the DNRA produced during spoofing is still:

- Session-specific
- Non-repeatable
- Non-transferable

Thus replaying the spoof output has no effect.

5.4.3 Eliminating Template Theft Implications

Even if biometric templates (or models) leak:

- They cannot regenerate past or future DNRA values
- They do not provide identity impersonation capability
- Their compromise does not imply system compromise

This is a **fundamental breakthrough in biometric security**.

5.5 Comparative Advantages Over FIDO2/Passkeys

FIDO2 and Passkeys store cryptographic secrets in secure hardware.
These secrets can be:

- Extracted
- Cloned
- Replayed
- Misused after device compromise

UDAS/DSS has no such secrets.
This makes it strictly superior in:

- Zero trust environments
- Cloud architectures
- IoT/robotic networks
- Industrial environments

UDAS/DSS is **not a competitor to biometrics or FIDO2**—
it is the **security layer they have always needed but never had**.

6. Formal Analysis of Security Properties

6.1 Confidentiality

Because no secrets are stored, confidentiality is achieved by design.
Compromise yields no meaningful data.

6.2 Integrity

DNRA is bound to session variables and entropy,
making it immune to modification without detection.

6.3 Non-Replay

Replay attacks fail because DNRA(S_1) is invalid in session S_2.
This is independent of time-based countermeasures.

6.4 Non-Impersonation

Without a secret to steal or mimic,
impersonation becomes mathematically infeasible.

6.5 Non-Residue Leakage

All components of DNRA vanish upon session termination.
No forensic artifact can reconstruct identity.

6.6 Mathematical Proof Sketches

We outline the following properties:

1. **Non-invertibility**
   f is designed such that $\nexists\ f^{-1}$ satisfying DNRA $\rightarrow$ inputs.
2. **Collision Impossibility**
   Given the dynamic entropy structure,
   $Pr[f(S_1) = f(S_2)] \approx 0$ for all realistic inputs.
3. **Unlinkability**
   $DNRA_1 \perp DNRA_2$
   (no mutual information exists).

7. System Architecture and Operational Flow

7.1 Client-Side Process

The client performs:

1. Biometric match (optional)
2. Collection of context & entropy
3. Generation of DNRA
4. Transmission of DNRA to the server

No key material is stored or reused.

7.2 Server-Side Verification Model

The server:

- Receives DNRA
- Independently derives expected values
- Validates via stateless computation

The server stores **no secret bound to user identity**.

7.3 Session Key Establishment

If required, a one-time session key can be derived from DNRA without ever storing any long-term key.

7.4 Stateless Validation Architecture

The system can be implemented across:

- Cloud environments
- Distributed networks
- Edge devices
- IoT clusters

No central secret store is required.

7.5 Hardware Independence Considerations

Unlike FIDO2 or secure-element dependent systems:

- No TPM
- No Secure Enclave
- No HSM

are required.

This dramatically reduces cost and increases scalability.

8. Use Cases and Applications

UDAS/DSS is not limited to a particular class of devices or environments.
Its architecture is general-purpose and highly adaptable.
Below we describe representative use cases demonstrating
the practicality and transformational potential of this approach.

8.1 Smartphones and Consumer Devices

Smartphones currently rely on:

- Biometrics (fingerprint, face)
- FIDO2 credentials
- Secure enclaves storing long-term secrets

These systems fail under device compromise, root access, or hardware extraction.

UDAS/DSS eliminates these risks entirely by ensuring:

- No secret is stored on the device
- No static credential exists to steal
- Biometric decisions cannot be replayed or exported
- Unlock artifacts are non-reusable and ephemeral

This allows smartphones to achieve **true zero-risk authentication**
for the first time.

8.2 Automotive and Mobility Systems

Connected vehicles utilize:

- Key fobs
- Digital keys
- Biometric access
- Vehicle-to-cloud authentication

All depend on static secrets, making them vulnerable to:

- Relay attacks
- Key cloning
- Signal amplification
- ECU impersonation

With UDAS/DSS:

- No authentication data can be replayed
- No long-term key exists to clone
- Biometric vehicle access becomes safe
- Vehicle-to-cloud authentication becomes stateless

This offers a **paradigm shift in automotive cybersecurity**.

8.3 Industrial Control and Robotics

Industrial devices often lack secure hardware, making stored secrets easy targets for malware or physical extraction.

UDAS/DSS benefits OT systems by:

- Eliminating shared keys across PLCs or robots
- Preventing impersonation of controller commands
- Enabling lightweight zero-trust architectures in factories
- Providing stateless authentication for constrained devices

This dramatically reduces the risk of industrial sabotage and robotic hijacking.

8.4 Cloud Identity and API Security

Current cloud security models heavily rely on:

- API keys
- OAuth tokens
- Service account credentials

These are the **most frequently leaked secrets in the world**.

UDAS/DSS removes this issue:

- Cloud services authenticate without storing secrets
- API calls carry non-replayable DNRA
- Zero-trust identity becomes mathematically enforced
- Secret rotation becomes unnecessary

This is particularly impactful for large-scale cloud systems and multi-tenant services.

8.5 Medical and Government Systems

Highly sensitive data systems require identity assurance without the risk of credential theft.
UDAS/DSS enables:

- Secure biometric access for medical staff
- Authentication without storing any reusable identifier
- Immutable audit trails of non-replayable authentication attempts
- High-assurance systems with minimal attack surface

This architecture aligns with strict regulatory environments
and national cybersecurity frameworks.

9. Implementation Considerations

9.1 Scalability

Because UDAS/DSS is stateless and does not depend on secure storage,
it scales horizontally across:

- Cloud clusters
- Edge networks
- IoT swarms
- Fog computing environments

No coordination or distributed secret management is required.

9.2 Latency Behaviors

UDAS/DSS computation consists of:

- Entropy collection
- Contextual binding
- DNRA generation
- Stateless verification

This results in **lower computational cost** relative to
cryptographic key exchange or certificate validation.

9.3 Key Management Absence and Its Advantages

Traditional systems require:

- Key rotation
- Secure transport

- Multi-party signing
- Revocation lists

UDAS/DSS simplifies this dramatically:

There are no keys to rotate, revoke, or store.

This eliminates an entire operational discipline.

9.4 Integration with Existing Standards

UDAS/DSS can complement or replace:

- FIDO2
- OAuth
- TLS client authentication
- Certificate-based systems
- Zero-trust identity layers

The architecture is protocol-agnostic and can be encapsulated within existing authentication flows.

9.5 Practical Deployment Scenarios

UDAS/DSS can be deployed in:

- Smartphones as a replacement for biometrics-to-server communication
- Cloud service APIs
- Autonomous robots
- Smart locks
- Vehicle telematics
- Industrial PLC networks

Its hardware independence makes adoption flexible and cost-effective.

10. Comparison With Existing Technologies

10.1 Biometric-Only Authentication

Weaknesses:

- Static templates
- Replayable match results
- Device vulnerability
- Irreversible compromise

UDAS/DSS resolves all these issues.

10.2 Token-Based Authentication

Tokens can be cloned, stolen, or replayed.
DNRA cannot be reused or reconstructed.

10.3 Certificates and PKI

PKI requires key storage, revocation lists, and secure hardware.
UDAS/DSS requires none of these and removes all PKI attack surfaces.

10.4 Zero-Knowledge Proof Models

ZKPs still depend on persistent secrets, unlike UDAS/DSS.
Thus, UDAS/DSS represents a fundamentally different model.

10.5 Why UDAS/DSS Is a New Class of Authentication

UDAS/DSS eliminates the following assumptions:

- Secrets must be stored
- Secrets must remain confidential
- Identity is proven with a persistent object

By breaking these assumptions, UDAS/DSS becomes:
the first authentication paradigm that eliminates credential theft at the root.

11. Discussion

11.1 Theoretical Implications

UDAS/DSS introduces a new foundation for authentication theory:
identity proof without secrets.
This has deep implications for cryptographic engineering,
security architecture, and AI–device trust systems

11.2 Impact on Cybersecurity Paradigms

UDAS/DSS shifts security models from:

- “Prevent leakage” → “Leakage is irrelevant”
- “Protect secrets” → “No secrets exist to protect”

- “Detect replay” → “Replay is mathematically impossible”

This dramatically alters system design philosophy.

11.3 Potential Limitations

We note:

- Requires robust entropy sources
- Protocol design must avoid predictable context
- Security guarantees depend on correct implementation of f

These are engineering considerations, not structural weaknesses.

11.4 Future Work Directions

Future research may include:

- Formal cryptographic proofs
- Hardware-accelerated implementations
- Large-scale cloud deployment case studies
- Integration with decentralized identity systems
- Automated DNRA parameter tuning using AI models

12. Conclusion

This paper introduced a new authentication paradigm, UDAS/DSS,
which eliminates stored secrets and generates one-time, non-reusable authentication artifacts. By integrating UDAS/DSS with biometric authentication,
we demonstrated the first mechanism capable of neutralizing
the structural weaknesses inherent in biometric systems.
The architecture enables:

- Stateless verification
- Non-replayable authentication
- Strong protection against impersonation
- Broad applicability across smartphones, cloud services, IoT, robotics, automotive systems, and critical infrastructure

UDAS/DSS represents a **foundational shift in authentication theory**
and a new direction for cybersecurity design.

We expect this model to significantly influence
future authentication frameworks and industrial practices.