Dynamic Non-Reusable Artifact (DNRA) Model
v2 (with Intuitive Overview)

Author: Yoshikazu Nakamura
Location: Aichi, Japan
Email: info@xinse.jp
Affiliation: Independent Researcher
Patent Application: JP2024-172823 (Patent Pending)

0. Intuitive Overview (Non-Technical Explanation)

This section is newly added in Version 2 to help general readers, executives, and non-technical stakeholders understand the core idea behind dynamic security.

0.1 What Is Dynamic Security?

Most security systems today rely on **static secrets** — things that do not change:

- A password
- A PIN code
- A fingerprint template
- A face recognition model

These stay the same every day.
If someone steals them, **they can be reused forever.**
Dynamic security introduces a completely different idea:

"A secret that exists only once, and disappears after use."

It is like having a key that works only one time, for one moment, and then turns into dust.

0.2 A Simple Example: 1210 → 1211

Imagine the following system:

- Today's password is **1210** (December 10).
- Tomorrow's password is **1211** (December 11).

If an attacker steals **1210**,
it becomes **completely useless** tomorrow.

This example is intentionally simple.
But it captures the true essence of dynamic security:
✓ **The key keeps changing**
✓ **A stolen key cannot be reused**
✓ **Yesterday's information has no value today**
Real dynamic security (DNRA/UDAS/DSS) does not use dates or simple numbers.
Instead, AI generates **trillions of unpredictable patterns**,
and each pattern is:

- Unique
- Non-reproducible
- Non-replayable
- Immediately discarded

But the "1210 → 1211" example helps people visualize the concept instantly.

0.3 Why Static Secrets Always Fail

Static authentication has one fatal weakness:
❌ **If it is stolen once, it is valid forever.**
This is true for:

- Passwords
- PINs
- Fingerprints
- Facial data
- Iris templates

Even biometric data — often marketed as "secure" — is actually **static**.
Your face, fingerprint, or iris **never changes**,
and once copied, it cannot be replaced.
This is why attacks on biometric systems are increasing every year.
Dynamic security solves this problem by ensuring:
"Even if stolen, the information is already obsolete."
Nothing static is valuable to an attacker.

0.4 How Dynamic Security Protects Biometric Data

Dynamic security allows biometric information to be transformed into:

A one-time, disposable authentication artifact.

This means:

- Your fingerprint is not reused.
- Your facial data is not stored as a static template.
- Each login produces a completely different one-time artifact.
- Even if someone copies your fingerprint image, it is **useless**.

In simple words:

Dynamic security makes biometrics "safe to steal,"

because the stolen version is already expired.

This is a revolutionary shift.

For the first time in history,

biometric authentication becomes **renewable** and **non-reusable**,

just like one-time passwords — but far more secure.

0.5 Why This Concept Never Existed Before

Before DNRA, the world had only two types of authentication:

1. **Static** (passwords, fingerprints, iris templates)
2. **Encrypted static** (same thing, just encrypted)

But encryption does not change the fact that the underlying data is static.

If the static data is compromised, the system fails.

No one had a method to generate:

- Secrets with no stored form
- Secrets that change every time
- Secrets that cannot be replayed
- Secrets that vanish immediately
- Secrets derived from biometrics but never stored

The DNRA model introduces **the world's first complete framework**

for generating such dynamic artifacts.

0.6 Summary of the Intuitive Concept

Dynamic security replaces:

❌ **"One key used many times"**

with

✅ **“New key every time, used once, then destroyed.”**

The 1210 → 1211 analogy explains this perfectly.

This intuitive concept prepares the reader for the technical details in the following sections.

Abstract

Static authentication systems—including passwords, PINs, and biometric templates—suffer from a structural flaw: once compromised, they remain permanently compromised. Biometric authentication, despite its widespread adoption, is fundamentally static and therefore vulnerable to irreversible leakage and spoofing attacks. This paper introduces the **Dynamic Non-Reusable Artifact (DNRA) Model**, a new authentication framework that generates **one-time, non-replayable, non-reversible, and non-storable dynamic artifacts** without relying on any static secrets. DNRA converts both digital inputs and biometric signals into unique, ephemeral authentication artifacts that cannot be reused or reconstructed, enabling *renewable* and *revocable* biometric authentication for the first time. Version 2 of this paper adds an intuitive overview to bridge understanding for non-technical audiences while maintaining technical rigor. DNRA eliminates entire classes of attacks—including replay attacks, template theft, biometric spoofing, AI-driven inversion, and database compromise—and represents a foundational shift from static to dynamic security in the future of digital identity.

Table of Contents

Part 2 — Technical Framework Sections (1–4)

Version 2 with Intuitive Overview

1. Introduction

The global authentication landscape has long relied on **static secrets**, such as passwords, PIN codes, and biometric templates. While these systems have been widely adopted, they suffer from a structural vulnerability:

❌ **Once a static secret is compromised, it remains compromised indefinitely.**

This fundamental limitation has resulted in billions of leaked credentials, persistent identity theft, and escalating biometric spoofing attacks. Biometric authentication, often assumed to be secure, is also static in nature—fingerprints, facial features, and iris patterns do not change. Once copied, they cannot be "re-issued."

To address this long-standing global security flaw, this paper introduces the **Dynamic Non-Reusable Artifact (DNRA) Model**, a new authentication framework capable of generating **non-reproducible, non-replayable, and non-storable one-time artifacts** without relying on any static secrets.

DNRA enables:

- Zero stored secrets
- Zero reusable templates
- Zero biometric leakage impact
- One-time, self-destructive dynamic artifacts
- Compatibility with both digital and biometric inputs

Version 2 of this paper adds **Section 0**, an intuitive explanation aimed at general readers and executives. The remainder of the document provides the formal technical foundation.

2. Limitations of Static Authentication Models

Traditional authentication systems treat identity as something that can be **stored**, **reused**, and **compared**. This approach is inherently flawed.

2.1 Static Password-Based Systems

Password systems rely on:

1. A stored static representation (hash or encrypted form)
2. A user-provided static secret for comparison

Weaknesses include:

- Predictability
- Replay attacks
- Database compromise
- User reuse across platforms
- Irrevocability once leaked

Even with hashing, the underlying model remains unchanged:

static in → static out → static comparison.

2.2 Static Biometric Systems

Biometric authentication is often misunderstood as inherently secure.

In reality:

- Fingerprints are static
- Facial features are static
- Iris patterns are static
- Voice signatures are static

Current systems convert these features into persistent templates.

Major weaknesses:

- Templates can be stolen
- Spoofing attacks are increasing
- Templates cannot be reset
- Biometric leakage is permanent

This violates a foundational security requirement:

✓ Any key must be revocable and replaceable

Biometrics fail this requirement by design.

2.3 Why Encryption Does Not Solve the Problem

Encryption protects data *in storage* or *in transit*, but:

- It does not change the static nature of the secret

- It does not prevent replay attacks
- It does not prevent template theft
- It does not prevent irrevocable compromise

Encrypted static data is **still static data**.

Therefore, static authentication models cannot be fixed through incremental improvements—they must be replaced.

3. Dynamic Non-Reusable Artifact (DNRA) Model

The DNRA Model proposes a new category of authentication:

Dynamic authentication with zero stored secrets and zero reuse.

DNRA transforms any user input—password, biometric pattern, behavioral signal—into a **unique, one-time authentication artifact** that:

- Exists only during the authentication moment
- Cannot be replayed
- Cannot be reversed
- Cannot be predicted
- Cannot be extracted or reconstructed
- Is mathematically and structurally non-reproducible

3.1 Core Principles

The DNRA framework consists of the following foundational principles:

(1) Zero Static Input Assumption

No raw input is ever used directly.

All inputs are processed through a dynamic transformation pipeline.

(2) One-Time Artifact Generation

Each authentication attempt produces a **unique artifact** that cannot be reused for a second attempt.

(3) Ephemeral Existence

Artifacts are destroyed immediately after evaluation.

(4) Non-Reversibility

Even full knowledge of the artifact yields no information about the user's input.

(5) Absence of Stored Secrets

No templates, hashes, or biometric profiles exist in storage.

3.2 Conceptual Architecture

DNRA consists of four stages:

1. **Input Abstraction Layer**
   Converts any raw signal (biometric or digital) into a dynamic intermediate representation.
2. **Entropy Expansion Layer**
   Expands input variability using AI-driven entropy enhancement.
3. **Artifact Synthesis Layer**
   Produces a non-reproducible dynamic artifact for this single session.
4. **Destructive Verification Layer**
   Verifies the artifact once and then irreversibly destroys it.

3.3 Non-Reproducibility Requirement

A DNRA artifact must satisfy:

- **Mathematical non-reproducibility**
- **Statistical non-repeatability**
- **Structural non-replayability**

Even if an attacker captures the entire artifact, it cannot be used again nor used to reconstruct the original input.

This property allows DNRA to defeat:

- Spoofing
- Replay attacks
- Biometric inversion attacks
- Database leaks
- Credential stuffing
- Template theft

4. Mathematical and System-Level Properties

The DNRA model is designed to satisfy strict theoretical constraints.

4.1 Non-Replayability

Given an artifact A_1 generated at time t_1:
A_1 cannot be reused at time t_2,
even by the legitimate system.
This differs from OTP (One-Time Passwords):

- OTPs depend on shared secrets
- DNRA has **no shared secrets**

4.2 Non-Reversibility

There exists no function f^{-1} such that:
input = f^{-1}(artifact)
Even with perfect knowledge of the artifact and system architecture,
the inversion problem remains unsolvable.

4.3 Destructive Evaluation

Once artifact A is evaluated, the system must ensure:
destroy(A) = true
No cache, log, or forensic method can recompute A.
This property is essential for:

- Zero stored secrets
- Zero forensic recovery
- Zero long-term risk exposure

4.4 Statistical Divergence Across Attempts

For any two authentication attempts using identical user input:
$D(A_1, A_2) \geq \delta$
Where δ is a required divergence threshold ensuring
artifacts remain **mathematically distinct** each time.
This enables the “dynamic” nature essential for biometric protection.

Part 3 — Sections 5 to Conclusion

Version 2 with Section 0 Intuitive Overview

5. Integration with Biometric Authentication

One of the most impactful applications of the DNRA model is the transformation of biometric authentication into a **dynamic, non-reusable system**. Traditional biometric frameworks rely on stored templates derived from the user's fingerprint, face, or iris. These templates are static and therefore vulnerable to theft, spoofing, and irreversible compromise.
DNRA enables a new paradigm:
Biometrics become dynamic, renewable, and inherently safe—even if stolen.

5.1 Eliminating Static Biometric Templates

Conventional biometric systems operate as:
raw biometric → static feature extraction → stored template → comparison
Weaknesses include:

- Templates can be extracted through database leaks
- Templates can be inferred from sensor side-channel attacks
- Templates can be reconstructed using generative AI
- Templates cannot be reset or replaced

Under DNRA, the pipeline changes fundamentally:
raw biometric → dynamic abstraction → entropy expansion → DNRA artifact
Critical differences:

- No template is stored
- No static representation exists
- Every login results in a distinct artifact
- A stolen artifact provides no value to attackers

5.2 Replay and Spoofing Immunity

Biometric spoofing attacks—synthetic fingerprints, AI-generated faces, 3D mask attacks—fail under DNRA because:
✓ **A successful attack today does not work tomorrow**
✓ **An artifact cannot be replayed**
✓ **Artifacts cannot be converted into templates**
✓ **System memory contains no long-term biometric data**
Static biometric systems compare expressions of the same template.
DNRA compares **dynamic relationships**, not static patterns.

5.3 Revocability and Re-Issuability of Biometrics

A long-standing issue in information security is:

❌ **Biometrics cannot be revoked.**

DNRA solves this by allowing the system to:

- Change the dynamic mapping rules
- Alter the entropy expansion function
- Modify the abstraction parameters
- Produce new artifact families

Thus, DNRA transforms biometrics into **revocable credentials**, a property previously considered impossible.

5.4 Mathematical Divergence for Biometrics

Even when the same fingerprint or face is used repeatedly, DNRA ensures that:

$D(A_1, A_2) \geq \delta\_bio$

Where δ_bio is a divergence constraint ensuring that biological inputs produce statistically distinct outputs on each authentication attempt.

This property protects against:

- Template averaging attacks
- Biometric inversion models
- Multi-sample inference attacks
- Cross-dataset linkage attacks

6. Security Analysis

The DNRA model is designed to satisfy core principles of modern cryptography and next-generation authentication requirements.

6.1 Resistance to Database Compromise

Since DNRA stores:

- no templates
- no hashes
- no biometric data

- no reusable artifacts

a database breach yields **zero actionable information**.

Even a full system compromise does not reveal:

- user identity
- valid authentication material
- reconstructable patterns

6.2 Resistance to AI-Driven Attacks

Modern attackers employ:

- Generative AI
- Predictive models
- Optimization-based inversion
- Large-scale correlation attacks

DNRA is naturally resistant because:

Artifacts provide no usable structure for AI to learn.

They are:

- Non-repetitive
- Non-correlated
- Non-reconstructable
- Non-generalizable

AI requires patterns; DNRA deliberately destroys patterns.

6.3 Zero-Knowledge Characteristics

DNRA approaches the behavior of zero-knowledge systems:

- The system learns nothing about the user
- The user exposes no reusable information
- Authentication succeeds without exchanging secrets

This aligns with the emerging paradigm of **trust-minimized identity**.

6.4 Attack Surface Reduction

DNRA eliminates entire classes of attacks:

✓ **Replay attacks**

✓ **Credential stuffing**

✓ **Template theft**
✓ **Biometric spoofing**
✓ **Brute force prediction**
✓ **Database leaks**
✓ **Cross-platform correlation**

Under static authentication, these risks are inherent.
Under DNRA, they are mathematically incompatible with the model.

7. Applications and Implications

DNRA is not merely an improvement to existing systems—it represents a **paradigm shift** in digital and biometric security.

7.1 Biometric Systems (Face, Fingerprint, Iris)

DNRA provides:

- Template-less authentication
- Spoof-proof verification
- Revocable biometrics
- Cross-device portability
- Safe biometric sharing

This is essential for:

- Smartphones
- Laptops
- Banking apps
- National ID programs
- Border control systems

7.2 Password-Free Authentication

DNRA allows truly passwordless systems:

- No static password exists
- Every login uses a unique artifact
- No credential theft possible

This is the natural successor to passwords, OTPs, and FIDO2.

7.3 High-Security Environments

Ideal for:

- Military-grade authentication
- Critical infrastructure
- Space systems
- Cloud identity platforms
- AI systems requiring identity validation

7.4 Identity Without Exposure

DNRA aligns with privacy-first and zero-trust models:

- No personal data is stored
- No biometric data is recoverable
- No cross-service tracking possible

User identity becomes **mathematically safe**.

8. Conclusion

The DNRA Model introduces the world's first complete framework for **dynamic, non-reusable authentication artifacts** that eliminate the inherent vulnerabilities of static secrets.

This paper showed:

- Static authentication cannot be repaired
- Biometrics are fundamentally insecure when static
- Dynamic artifacts solve these structural problems
- DNRA makes biometrics safe, renewable, and spoof-resistant
- Zero stored secrets eliminate database compromise risks
- AI-driven attacks become ineffective
- Authentication can finally become both secure and private

Version 2 adds an intuitive overview, enabling broader understanding while maintaining full technical rigor.

DNRA represents a significant milestone:

The transition from static to dynamic security—

a foundational shift for the future of digital identity.