Dynamic Code Authentication

A DNRA-Based Security Framework for QR and Barcode Systems

Version 3 (V3)

Author: Yoshikazu Nakamura
Location: Aichi, Japan
Email: info@xinse.jp
Affiliation: Independent Researcher

Patent Application: JP2024-172823 (Patent Pending)

Abstract

Static QR codes and barcodes are foundational components of modern digital and physical infrastructure, enabling payments, ticketing, logistics, authentication, and consumer interactions.

However, their static nature introduces critical vulnerabilities: they can be copied, replaced, photographed, modified, and reused without limitation. These structural weaknesses have led to widespread security incidents such as QR code replacement fraud, malicious URL redirection, counterfeit product labeling, and unauthorized ticket duplication.

This paper introduces **Dynamic Code Authentication (DCA)**, an application of the **Dynamic Non-Reusable Artifact (DNRA)** security model, enabling QR codes and barcodes to operate as *dynamic, single-use, non-replayable authentication artifacts*. Unlike static approaches, DCA requires **no new hardware**, **no specialized scanners**, and **no user-side burden**, since the dynamic artifacts are encoded directly into standard QR or barcode formats. All existing scanning devices—including smartphones, POS scanners, and logistic readers—continue to function without modification. Only the server-side validation logic becomes dynamic.

We present an intuitive explanation of dynamic codes, a threat analysis of static identifiers, the mathematical and architectural principles behind DNRA, and detailed integration models for QR and barcode ecosystems. We demonstrate that dynamic codes eliminate all major attack vectors—including replacement, duplication, replay, URL substitution, and offline copying—while maintaining full backward compatibility.

Dynamic Code Authentication represents a critical step toward universal secure identification in payments, logistics, healthcare, government systems, and global commerce. By transforming the world's most widely deployed identification formats into dynamic authentication channels, DNRA enables the next-generation security layer for both digital and physical environments.

Collaboration and Partnership Invitation

The author is actively seeking collaboration with qualified organizations that recognize the strategic value of Dynamic Security Systems, Dynamic QR/Barcode Authentication, and Dynamic Biometric Protection.

Partnership opportunities include **research collaboration, joint development, technology licensing, or full acquisition of the underlying intellectual property**.

Due to the broad applicability of this technology—ranging from financial security and digital identity to payment systems, logistics, healthcare, and IoT infrastructure—early engagement may provide a significant competitive advantage to participating companies.

Organizations interested in evaluating the technology, discussing potential partnerships, or exploring exclusive licensing arrangements are invited to contact the author directly:

Author: Yoshikazu Nakamura
Email: info@xinse.jp

All discussions can be conducted under NDA upon request.

Table of Contents

0. Intuitive Overview: Understanding Dynamic QR and Barcode Security

To understand Dynamic Code Authentication, imagine a simple idea:

A code that is valid only "right now" and becomes useless the moment someone tries to reuse it.

Static QR codes and barcodes behave like fixed passwords printed on paper:

- If someone photographs them, they work.
- If someone copies them, they work.
- If someone replaces them, they work.

This is why QR replacement fraud, malicious URL embedding, and barcode counterfeiting continue to increase worldwide.

Now imagine a different world:

- A QR code that changes every moment.
- A barcode that becomes invalid as soon as it is scanned once.
- A copied or photographed code that simply does not work.
- A replaced code that servers instantly reject.

This is the idea behind **Dynamic QR Codes** and **Dynamic Barcodes**.

Even more importantly:

No new scanners or user devices are required.

Only the security logic becomes dynamic, not the scanning equipment.

A supermarket scanner will read a dynamic barcode exactly as before.

A smartphone camera will read a dynamic QR code exactly as before.

The *difference* is how the server interprets the value:

Instead of checking whether the code "matches a stored value,"

the server checks whether the value is **a valid DNRA artifact** generated in real time.

This means:

- Stolen codes are useless.
- Copied codes are useless.
- Modified codes are useless.
- Old screenshots are useless.

- Fraudulent replacement codes are instantly rejected.

In short:

Dynamic codes behave like a living ID that cannot be reused, copied, or forged.

This simple principle eliminates nearly every known attack on QR and barcode systems without altering the devices people already use.

1. Introduction

QR codes and barcodes form the backbone of global identification infrastructure.

They are used in:

- retail and inventory management
- logistics and supply chains
- healthcare and medication tracking
- mobile payments
- event ticketing
- identity verification
- transportation systems
- smart city applications

Despite their ubiquity, both systems rely almost entirely on **static identifiers**.

A static code remains valid until someone intentionally changes it—

and criminals exploit this property every day.

Recent years have seen a surge in incidents such as:

- QR code replacement at restaurants and stores
- Fake payment QR codes layered over legitimate ones
- Malicious URLs embedded into counterfeit QR stickers
- Counterfeit barcodes placed on products
- Ticket duplication and unauthorized reuse
- Barcode relabeling in logistics systems

These vulnerabilities arise not because QR or barcodes are flawed technologies,

but because **static identification is fundamentally insecure** in the modern environment.

The DNRA (Dynamic Non-Reusable Artifact) security model provides a

powerful solution:
turn codes—any codes—into **dynamic, single-use authentication artifacts**.
By applying DNRA to QR and barcode formats, we obtain:

- Dynamic QR Codes
- Dynamic Barcodes
  → both requiring no new hardware, no special scanners, and no additional user burden.

The remainder of this paper explores the limitations of static identifiers,
the conceptual and mathematical basis for dynamic codes,
and the practical integration pathways for global QR and barcode ecosystems.

2. Limitations of Static QR and Barcode Models

QR codes and barcodes were originally designed as *identifiers*, not as *security mechanisms*.
Their purpose was to store fixed information in a compact optical format. While this made them highly versatile and widely adopted, it also introduced severe security limitations that become critical in modern use cases.

2.1 Copyability and Unlimited Reuse

A static QR code or barcode can be:

- photographed
- printed again
- screenshotted
- replicated with any printer
- stored and reused indefinitely

This property is convenient for distribution, but dangerous for authentication.

2.2 Replacement Attacks

The most common QR-based fraud:
A criminal simply places a fake QR sticker over a legitimate one.
Victims scan the malicious code and unknowingly:

- send payments to a criminal-controlled account
- visit phishing websites
- download malware
- submit credentials to fraudulent portals

Because static QR codes contain fixed data, scanners cannot detect the tampering.

2.3 Malicious URL Embedding

A QR code containing a URL can be replaced with one pointing to:

- malware
- phishing pages
- impersonation login portals
- fake payment pages

Static codes provide no cryptographic or contextual verification.

2.4 Ticket and Access Counterfeiting

Tickets, access passes, and coupons commonly use QR or barcodes.

Static codes enable:

- duplication
- resale
- forging
- unauthorized sharing
- unlimited reuse until detection

This results in massive financial losses.

2.5 Supply Chain and Barcode Fraud

In logistics, barcodes are used to track:

- inventory
- food distribution
- medication
- industrial components
- shipping containers

Static barcodes allow:

- relabeling
- product substitution
- counterfeit goods entering supply chains
- unauthorized redirection of shipments

2.6 Structural Source of All Vulnerabilities: “Static” Data

Every attack shares a single root cause:

Static identifiers cannot defend themselves.

If copied, they still work. If replaced, scanners accept them.

The modern security landscape requires identifiers that *change*, *expire*, and *cannot be replayed.*

This leads to Dynamic Code Authentication.

3. Dynamic Code Authentication (DCA) Framework

Dynamic Code Authentication applies the DNRA (Dynamic Non-Reusable Artifact) security model to QR and barcode systems.

This transforms codes from static identifiers into **dynamic, single-use authentication tokens**.

3.1 Core Concept

Instead of encoding fixed data, a dynamic code contains a DNRA artifact:

- generated in real time
- valid only in a specific context
- non-reusable
- non-replayable
- non-reversible
- non-storable

A dynamic QR/barcode scanned twice will succeed once and fail subsequently.

3.2 Why No New Hardware Is Required

QR codes and barcodes are merely *containers* for alphanumeric data.

A DNRA artifact is also just data.

Therefore:

- A smartphone camera reads the code normally.
- A supermarket scanner reads the code normally.
- A logistics barcode reader reads the code normally.

The *interpretation* changes, not the hardware.

This compatibility is the strongest advantage of DCA.

3.3 How Dynamic Codes Are Generated

A dynamic QR or barcode contains:

DNRA("context", timestamp, local factors, entropy)

Examples of context:

- payment session

- ticket ID
- shipment ID
- device pairing request

The resulting artifact is encoded into QR or barcode format.

3.4 How Validation Works

The server checks:

1. Was this artifact generated for this context?
2. Is the timestamp valid?
3. Has it already been used?
4. Is the artifact mathematically correct under DNRA rules?

If any fails → the code is rejected.

3.5 Why Attacks Become Impossible

Dynamic codes resist:

- copying → artifact becomes invalid
- replacement → artifact does not match context
- replay → timestamp mismatch
- URL injection → URLs no longer used as identifiers
- barcode relabeling → each scan must match DNRA rules

In effect:

DCA makes code-based fraud structurally impossible.

4. Mathematical and System-Level Properties

This section summarizes the formal properties of DNRA as applied to QR and barcode formats.

4.1 Non-Reusability

Each artifact is tied to:

- timestamp
- entropy
- context

Once validated, it is marked as used.

4.2 Non-Replayability

Even if intercepted:

- the timestamp is obsolete

- the server rejects any “previous” artifact
- copying the code produces immediate failure

4.3 Non-Reversibility

DNRA artifacts contain no reversible pattern.

An attacker cannot derive secrets, keys, or context from the output.

4.4 Non-Storable Architecture

Servers maintain no static passwords or keys.

Validation is based on dynamic rules, not stored secrets.

This eliminates the risk of:

- database leaks
- credential theft
- static key compromise

4.5 Contextual Binding

An artifact is valid *only for its designated purpose*, e.g.,

- the exact payment amount
- the exact ticket session
- the exact product batch
- the exact container ID

Context mismatch → automatic rejection.

4.6 Compatibility with Global Standards

DNRA artifacts can be encoded into:

- QR Model 1 / Model 2
- Micro QR
- DataMatrix
- EAN-13 / UPC-A
- Code 39 / Code 128
- GS1 supply chain formats

This ensures deployment across all industries.

5. Integration with QR Code Systems

QR codes are widely used in payments, advertising, ticketing, logistics, and identity systems.

Their static nature has caused a surge in fraud globally.

Dynamic QR Codes resolve these problems without altering the scanning experience.

5.1 Preventing Replacement Attacks

Fake QR stickers become useless because:

- the dynamic artifact must match server-side rules
- replaced codes never match the expected context
- the server rejects fraudulent artifacts instantly

5.2 Eliminating Malicious URL Attacks

Dynamic QR does not contain raw URLs.

Instead:

dnra://artifact

The server determines the correct destination.

Attackers cannot embed malicious links.

5.3 One-Time Ticketing and Access Control

Dynamic QR enables:

- single-use tickets
- non-duplicable event passes
- time-bound transit access
- secure temporary authentication

No duplication or resale is possible.

5.4 Seamless User Experience

Scanning looks the same:

- same camera
- same app
- same behavior

Only the security becomes dramatically stronger.

6. Integration with Barcode Systems

Barcodes remain the global standard in:

- retail
- manufacturing
- logistics
- healthcare

- warehousing

Dynamic barcodes offer immediate enhancements.

6.1 Anti-Counterfeit Protection

Product barcodes can be made dynamic at packaging time or distribution points.

This prevents:

- replication
- relabeling
- counterfeit goods entering supply chains

6.2 Secure Logistics Tracking

Each scan updates the artifact, ensuring:

- correct path
- no unauthorized diversion
- tamper detection

6.3 Preventing Ticket or Coupon Reuse

Barcodes used for:

- movie tickets
- amusement parks
- transportation
- coupons

become one-time identifiers under DNRA.

6.4 Backward Compatibility

All existing barcode scanners—including old laser models—
can read dynamic barcodes because they behave like ordinary text identifiers.

7. Security Analysis

This section analyzes Dynamic Code Authentication (DCA) using standard adversarial models.

We evaluate the system against existing QR and barcode attack vectors and demonstrate that DNRA-based dynamic codes eliminate vulnerabilities inherent to static identifiers.

7.1 Threat Model

We consider attackers capable of:

- copying or photographing QR/barcodes
- printing counterfeit codes
- replacing legitimate codes with malicious ones
- relabeling products or packages
- embedding malicious URLs
- conducting replay attacks
- intercepting codes during transmission
- performing offline brute-force attempts

We assume the attacker has no access to DNRA generation rules or server-side validation logic.

7.2 Attack Resistance Evaluation

Replacement Attacks → Defeated

Dynamic codes cannot be replaced by static substitutes because:

- server validation checks context
- timestamps make old or forged artifacts invalid
- replaced codes never align with expected DNRA output

Even visually identical fakes fail cryptographically.

Copying / Duplication → Defeated

A copied dynamic code fails because:

- once used, the artifact is marked invalid
- timestamp windows prevent reuse
- entropy prevents prediction

Screenshots, photos, and printed copies become ineffective.

Replay Attacks → Defeated

Replaying a previously scanned code fails due to:

- time expiration
- one-time validation
- server-side “used artifact” tracking

This property directly eliminates the fundamental weakness of static QR and barcodes.

Malicious URL Attacks → Defeated

Dynamic QR does not embed URLs.

Instead, the server interprets:

dnra://artifact

Therefore:

- attackers cannot redirect users
- malicious links cannot be substituted
- phishing via QR becomes impossible

This closes a major global attack vector.

Barcode Relabeling / Product Counterfeiting → Defeated

Dynamic barcodes eliminate:

- counterfeit goods with copied labels
- unauthorized rerouting of items
- tampered medication packaging
- black market substitution

Each scan must match a valid DNRA artifact tied to the product's true context.

Database Theft Resistance

Because DCA uses:

- non-stored secrets
- non-reversible artifacts

even a full server database leak provides no reusable authentication material.

AI-Based Attacks → Defeated

Modern generative AI can replicate static patterns easily.

However, DNRA artifacts:

- lack any reversible structure
- include entropy and contextual elements
- operate under one-time validation rules

Therefore, neither AI nor classical cryptanalysis can reconstruct valid artifacts.

8. Applications and Global Implications

Dynamic Code Authentication can be deployed anywhere QR or barcodes are used today—
which encompasses nearly every sector of the global economy.

8.1 Payments and Fintech

Dynamic QR enables fraud-proof transactions:

- secure mobile payments
- merchant-to-customer QR integrity
- donation systems
- public service payments

No replacement attack can succeed.

8.2 Ticketing and Access Control

Dynamic QR/barcodes support:

- single-use tickets
- event passes
- transportation systems
- access keys for secure facilities

Counterfeiting becomes impossible.

8.3 Logistics and Supply Chain

Dynamic barcodes ensure:

- tamper detection
- anti-counterfeit packaging
- authenticated hand-off events
- secure container routing
- food and medicine safety

This significantly strengthens global supply chain integrity.

8.4 Retail and Product Authentication

Retailers benefit from:

- anti-relabelling protection
- counterfeit prevention
- secure discount coupons
- verified product origins

Backward compatibility ensures no hardware changes are needed.

8.5 Healthcare and Medication Tracking

Dynamic barcodes prevent:

- incorrect patient-label pairing
- medication substitution
- fraudulent reuse of medical forms
- forged laboratory results

This has substantial life-saving potential.

8.6 Government, Smart Cities, and Identity

Applications include:

- resident ID authentication
- temporary permits
- parking systems
- municipal services
- immigration and border control
- disaster response coordination

Dynamic codes eliminate identity and access misuse.

8.7 Global Standardization Potential

Because QR codes and barcodes are universal,
introducing dynamic variants could lead to:

- new ISO/IEC standards
- next-generation GS1 formats
- international adoption in finance and shipping
- government-level security requirements

DCA may become a new **global authentication layer**, reshaping secure identification.

9. Conclusion

Static QR and barcode systems, while ubiquitous, suffer from inherent vulnerabilities: they can be copied, replaced, replayed, and misdirected. These weaknesses have resulted in financial loss, security breaches, supply chain disruptions, and widespread fraud.

Dynamic Code Authentication, powered by the DNRA security model, resolves these vulnerabilities at their root by transforming codes into dynamic, single-use authentication artifacts. This transformation requires **no new hardware**, **no special user devices**, and **no changes to scanning behavior**. Existing QR and barcode infrastructure can continue operating normally while gaining a mathematically secure, tamper-proof authentication layer.

As global dependence on code-based identification grows, the transition from static to dynamic systems becomes both logical and inevitable. DCA provides a practical, scalable, and backward-compatible pathway for securing the world's most widely deployed identification technologies.

Dynamic QR and Dynamic Barcodes represent a natural extension of DNRA principles—bringing dynamic security to everyday code systems and enabling a safer digital and physical world.

Acknowledgments (optional)

This work expands upon the DNRA security model and its foundational theory. Special recognition is given to the development of Dynamic Security Systems that enable universal, context-aware, non-replayable authentication mechanisms.