A powerful mix of security, privacy & trust for NFC in today's IoT

These highly secure and remarkably powerful NFC tags protect data while enabling advanced functionality, so businesses can introduce smart, digitally connected products for trusted applications at scale.

NTAG 424 DNA | NTAG 424 DNA TAGTAMPER
SECURE NFC TAGS

KEY FEATURES

- Full NFC interoperability: ISO/IEC 14443-A communication, NFC Forum Type 4 Tag
- 416 bytes memory organized in an ISO/IEC 7816-4 file system: 32 bytes capability container, 256 bytes NDEF file, 128 bytes protected data file
- Common Criteria EAL4 certification
- Standard AES-128 cryptography for authentication/secure messaging, or LRP-wrapped AES operation for even higher attack resistance
- SUN message authentication for advanced data protection within standard NDEF read operation
- 3-pass mutual authentication to access protected data file
- Protected communication on contactless air interface
- ECC-based NXP originality signature and LRP-based NXP originality check for assurance of tag origin
- Random ID and encrypted UID for enhanced privacy
- On-chip assembly of item URLs with flexible ASCII mirrors
- Ultra-fast communication (up to 848 Kbits/s), benchmark authentication time
- High input capacitance (50 pF) for compact antenna design
- Optional tamper loop for once-opened and current-status detection (NTAG 424 DNA TagTamper)

KEY BENEFITS

- Cryptographically secure message authentication with any standard NFC phone
- On-chip sensitive data storage with tag-reader mutual authentication & encrypted data transfer
- Supports latest regulations for privacy protected user data
- Authentication in near real time, for intuitive, convenient user experience
- Optional anti-tampering with on-chip status detection (NTAG 424 DNA TagTamper)

APPLICATIONS

- Advanced anti-counterfeiting
- Secure supply-chain traceability and authorized data access
- Exclusive, hyper-personalized content and experiences
- Trusted offers for vouchers, loyalty coupons, etc.
- Authenticated documents
- Auditable trail of presence
- Tamper proofing (NTAG 424 DNA TagTamper)
- Status-driven messaging pre/post retail (NTAG 424 DNA TagTamper)

Near Field Communication (NFC) is a foundational technology in consumer and industrial segments of the Internet of Things (IoT). NFC is a trusted, intuitive way to perform identification, authentication, and localization, and is supported by every major smartphone manufacturer. NFC also enables new capabilities throughout a product's life cycle, from provenance, manufacturing, brand protection, and supply-chain control to retail, consumer experiences, and more. Security is an essential part of NFC functionality because, if assets and data are not adequately protected, IoT-connected applications can be vulnerable to IP theft, tampering, data breaches, and other types of abuse.

With the NTAG 424 DNA NFC tags, NXP sets new standards for security, privacy, and trust for NFC in today's IoT.

The NTAG 424 DNA offers special security features, such as AES-128 cryptographic operation and the new SUN message authentication mechanism, along with sensitive data protection with granular access permissions. Moreover, the NTAG 424 DNA TagTamper adds an anti-tampering function with on-chip status detection.
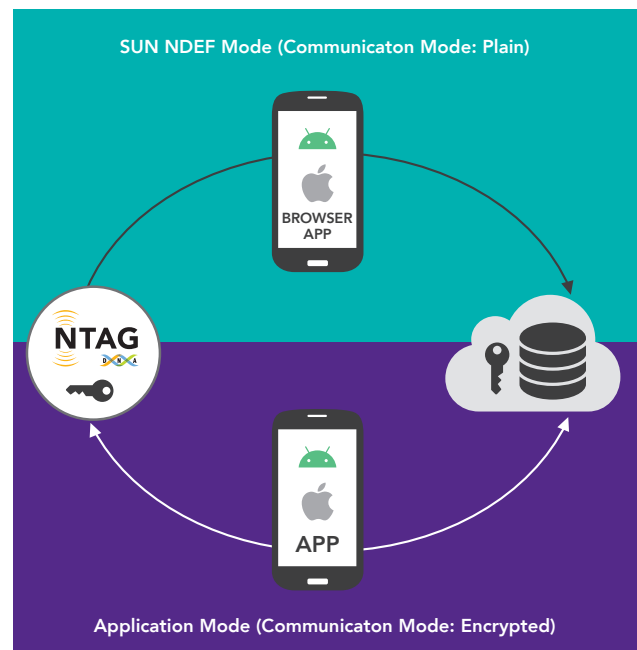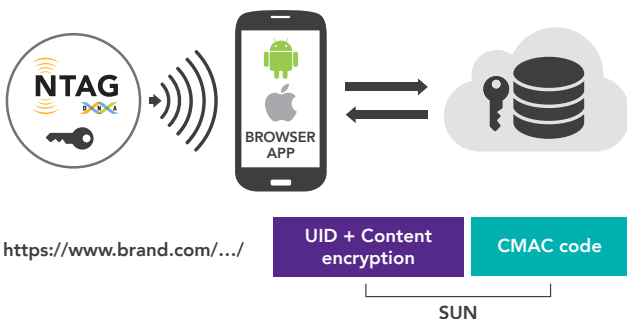
The high level of security and extensive feature set make these tags uniquely positioned to protect assets while enabling a new generation of hyper-personalized user experiences, delivered in near real time.

MULTI-LAYERED PROTECTION

The NTAG 424 DNA architecture supports AES-128 based encryption with five customer-defined keys. AES-128 cryptography is used by governments worldwide for authentication and secure messaging. In addition to the standard implementation, there is an optional AES-based protocol that uses a Leakage Resilient Primitive (LRP), which increases attack resistance even further.

SUN MESSAGE AUTHENTICATION

Each time an NTAG 424 DNA tag is tapped, it generates a Secure Unique NFC (SUN) authentication message using an AES-128 cryptogram. An NFC-enabled device reads the tap-unique URL with its crypto-secure SUN code, sends it to the server for secure tag and message authentication, and returns the verification result. The SUN mechanism in NDEF mode is compatible with all standard NFC phones, and offers a more secure way to maintain data confidentiality and integrity.

SUN NDEF Mode (Communicaton Mode: Plain)

Application Mode (Communicaton Mode: Encrypted)

https://www.brand.com/.../

| UID + Content encryption | CMAC code |

SUN

SUN HIGH-LEVEL STORAGE SECURITY

Fine-grained permissions ensure that only authorized users, applications, and devices can access sensitive data or issue commands. Valid mutual authentication uses a two-way, encryption-based scheme for the reader and tag to authenticate each other at the same time, and data remains encrypted over the contactless interface. This works in Application mode. The result is end-to-end protection from the tag to the reader and the server.

> **9 billion data records have been lost or stolen since 2013, but only 4% are 'secure' breaches where encryption was used to render such data useless. (Breach level index, Gemalto)**
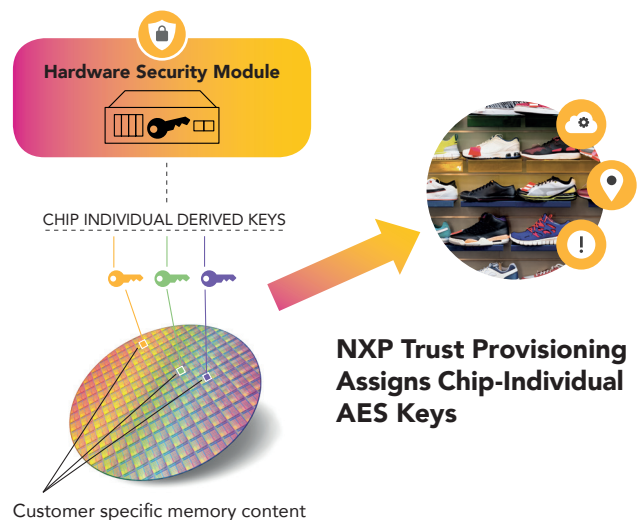
PRIVACY REGULATIONS

Special on-chip features, including the random ID and optional UID and data encryption for SUN, let NTAG 424 DNA tags demonstrate accountability for personal data, as now required in many regions of the world.

OPTIONAL TAMPER PROTECTION

The NTAG 424 DNA TagTamper includes a tamper loop, to detect if a product has been mishandled or opened before the sale. A quick read of the tag status verifies that the loop is intact, to confirm product integrity. The two-stage status message is securely protected against manipulation.

VALUE-ADDED SECURITY SERVICES

A complete suite of value-added services enhance system security. The NXP Trust Provisioning Service creates and provisions chip-individual AES keys, derived from master keys in FIPS 140-2 Level 3 certified Hardware Security Modules (HSM). These are used in NXP's secure manufacturing facilities to insert diversified keys and data into individual tag ICs. The NXP Encoding Service securely encodes customer-specific NFC tag data at ultra-high speeds during manufacturing. NXP's cloud-based NFC Authentication Service supports advanced cryptographic operations. NFC Authentication & Redirection is a robust authentication engine with tag-management capabilities, and the NFC Standalone Authentication lets customers manage their own tags while relying on NXP for added security. A free set of purpose-built software tools

Hardware Security Module

CHIP INDIVIDUAL DERIVED KEYS

NXP Trust Provisioning Assigns Chip-Individual AES Keys

Customer specific memory content

simplifies system integration, and two plug-and-play solutions, the TapLinx SDK for Android, iOS, and Desktop, and the NFC Reader Library, make application development fast and easy.

THE NEXT LEVEL OF TRUSTED APPLICATIONS

NTAG 424 DNA tags use multi-layered security to support a broad range of NFC-based applications that can be trusted to protect products, services, and user experiences.

COMBAT COUNTERFEITING

Protect against losses by verifying a product's authenticity, anytime, anywhere in the world. Improve accountability for provenance and increase customer confidence. Consider mobile authentication and automated authentication for embedded devices, enabled by a secure reader and a tagged refill or replacement item.

CONTROL YOUR SUPPLY CHAIN

Securely authenticate products at any time, during sourcing, manufacturing, distribution, chain of custody, or brand protection. Safeguard tag data through access-protected memory to let authorized staff securely read production data, log payment incidents, or customize product-related data.

ENABLE NEXT-GEN USER EXPERIENCES

Evolve the customer experience by engaging more dynamically and with greater personalization. Reward customers for purchases and make ownership more valuable with individualized services, exclusive loyalty rewards, and unique buying privileges.
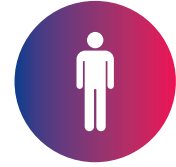
VERIFY PHYSICAL PRESENCE

Enable secure visitor authentication, with proof of presence and confirmation of visit details. Provide trust, with an auditable tag presence and data logs, for personnel in equipment maintenance, repair workers, field inspectors, security guards, and more.

PROTECT MONEY OFFERS

Ensure authenticity of coupons and gift vouchers to avoid counterfeits. Support digital promotions and loyalty offers while preventing misuse, by securing one-time-use URLs.

AUTHENTICATE DOCUMENTS

Quickly confirm the originality and provenance of important documents that bear specific IDs and credentials, such as certificates of authenticity, deeds of trust, marriage and birth certificates, diplomas, and other legal documents.

DETECT TAMPERING

Let inspectors and consumers securely detect whether a product has been interfered with or opened prior to sale, anywhere in the supply chain, using tamper-evident labels, seals or closures. (NTAG 424 DNA TagTamper)

TRIGGER STATUS-BASED MESSAGES

Use product status to prompt targeted marketing messages. Pre-sale messages can include product provenance, helpful information, reviews, while post-sale messages can include services, loyalty rewards, e-commerce, and more. (NTAG 424 DNA TagTamper)

ORDERING INFORMATION

	Product type	12NC	Delivery form & Quantity	Input Capacitance
NTAG 424 DNA	NT4H2421G0DA8	9353 776 94118	MOA8 Module	50pF
	NT4H2421G0DUD	9353 776 93003	Sawn wafer 120µm, MOQ: 1 wafer	50pF
	NT4H2421G0DUF	9353 777 69003	Sawn wafer 75µm, MOQ: 1 wafer	50pF
NTAG 424 DNA TAGTAMPER	NT4H2421TTDUD	9353 777 71003	Sawn wafer 120µm, MOQ: 1 wafer	50pF
	NT4H2421TTDUF	9353 777 72003	Sawn wafer 75µm, MOQ: 1 wafer	50pF

www.nxp.com/nfc

Common Criteria
CERTIFIED EAL4

NTAG
DNA