CREATE STRONG, SECURE, CONNECTED PRODUCTS:

NXP Delivers Unmatched Protection & Scalability with New **NFC Services for the NTAG Product Family**

STRONG. SECURE. CONNECTED.

Near Field Communication (NFC) technology is a gateway to the digital era, giving you more ways to strengthen your brand, protect your customer experiences, and control your operations. Equipped with digital NFC and Internet of Things (IoT) capabilities, physical items become uniquely identifiable, interactive, and traceable, so they protect value at every point of the product life cycle, from the point of manufacture to the consumer's hand.

On-item NFC electronics connect products to the web, by simply tapping them with a smartphone, or by placing them on or near smart reader devices. The IoT securely collects IDs and data from these devices and communicates that information to the cloud, where products have their own addressable digital profiles and can exchange data in real time.

At NXP, we bring our deep experience in high-security applications, including eGovernment, payment, and access, to the design of our NFC smart tagging products, so we're uniquely positioned to offer best-in-class solutions for digital authentications and secured customer experiences. Our aim is to offer true end-to-end secure solutions, with the help from tags and the cloud, so you can match protection to your specific product and supply chain needs, while easing integration into existing platforms.
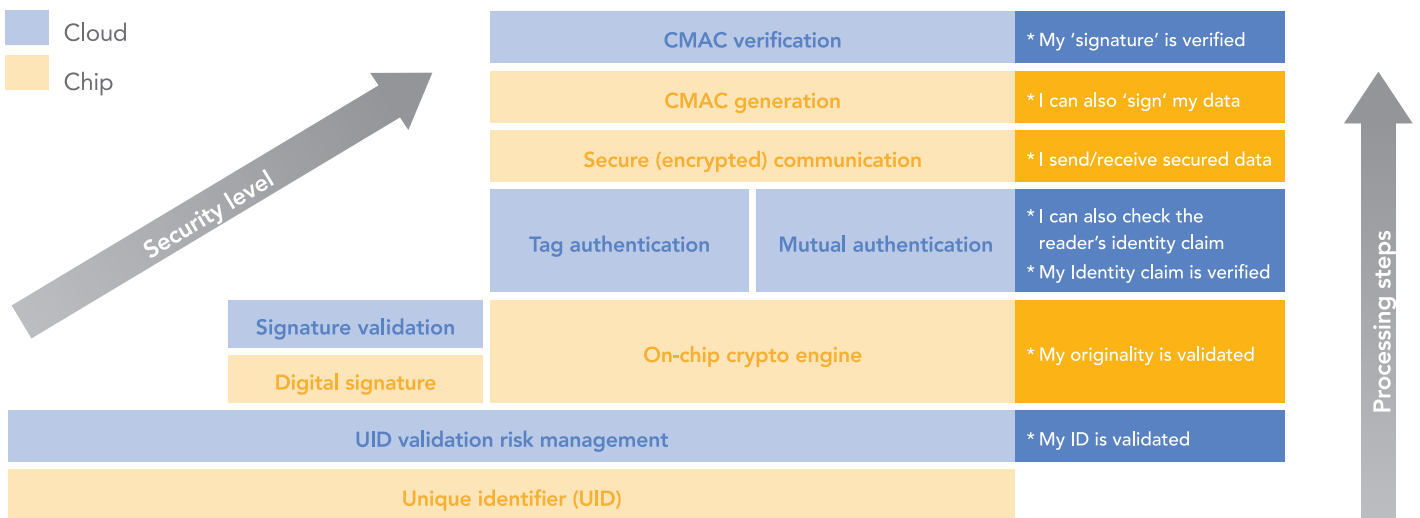
NXP – THE BEST IN NFC TECHNOLOGY

Physical products face ongoing threats by persistent counterfeiters armed with increasingly sophisticated tools. As the Identification industry's number-one supplier of semiconductor technology, NXP has assembled an extensive portfolio of **NTAG NFC products** with different levels of on-chip security features, from base level to cryptography, with or without tamper evidence, so you can always find the right fit for your application.

On-chip security features serve as fundamental enablers for brand protection but benefit from the broader support offered by secure software. Consequently, the trend toward hardware- and cloud-enabled security emerges as the most promising solution underlying the explosive growth of interconnected applications.

Security by Design

From base level to cryptographic operations

NTAG   **NTAG** DNA

- Cloud
- Chip

Security level →

|		
CMAC verification		* My 'signature' is verified
CMAC generation		* I can also 'sign' my data
Secure (encrypted) communication		* I send/receive secured data
Tag authentication	Mutual authentication	* I can also check the reader's identity claim * My Identity claim is verified
Signature validation / Digital signature	On-chip crypto engine	* My originality is validated
UID validation risk management		* My ID is validated
Unique identifier (UID)		

Processing steps →

Our most advanced **NXP DNA** product line – **NTAG® 424 DNA** and **NTAG 424 DNA TagTamper** - includes AES-128 hardware for cryptographic operations on attack-resistant silicon. The DNA products use symmetric cryptography, with the same key for encryption and decryption, to safeguard information. The main advantage of symmetric algorithms is their efficiency and speed of execution, to manage digital signing and authentication applications.

NFC

NTAG CONFIGURE & TRUST

NTAG Configure & Trust is a Chip Customization service, resulting in chip products that are ready to use as shipped. NXP encodes customer-specific tag data at ultra-high speeds during wafer manufacturing, so customers benefit from high cost-efficiencies.

Inevitably, application and system security depend on preserving the secrecy of the all-important crypto keys. To strengthen the security of end applications, NXP provides a Trust Provisioning service along with its NTAG DNA crypto products. This includes creation and provisioning of die-individual keys in Hardware Secure Modules (HSM) in a FIPS 140-2 Level 3 compliant certified environment, whereby only these HSMs have access to master secrets. The keys and die-individual data generated by the HSMs are inserted into each chip during the production flow in our secure manufacturing facilities.

Hardware
Security Module

Chip individual
derived keys

Customer specific
memory content
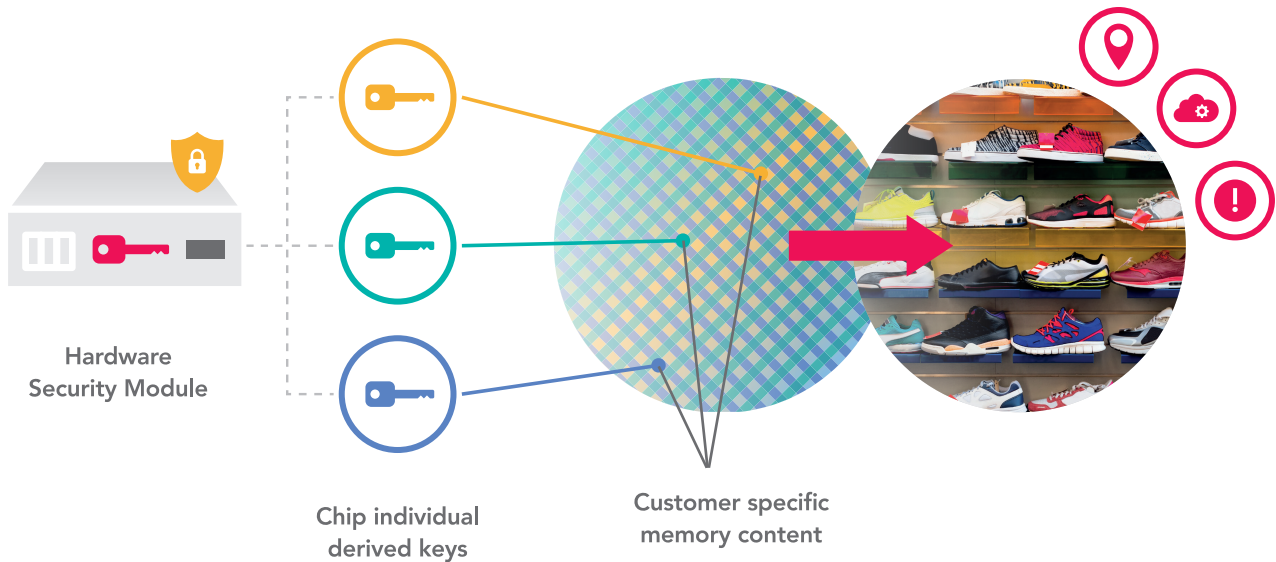
Whenever a key exchange is required (for example in case of a customer key transfer to NXP) it is done with encryption, using a secure communication channel to protect the master secret against malicious attacks or breaches.

NTAG SECURE CLOUD SERVICES

To make our technology as easy to use as possible, NXP has developed NTAG Secure Cloud Services. Our services are remarkably flexible and scalable for managing, protecting and controlling billions of IoT product identities in the cloud, giving each product a persistent, addressable web presence, to exchange data in real-time.

Encoded chips (also available as NXP Standard Products) are converted into tags and attached to physical products. Our NTAG Validator & Redirector links products to your own content platform, enabling faster time to market for uniquely connected digitized products. Trusted risk management for NTAG baseline products can be enabled, where blacklists are generated according to certain criteria.

In combination with our higher-security products, such as NTAG 424 DNA and NTAG 424 DNA TagTamper, you benefit from a robust authentication engine, within our NTAG Authenticator & Redirector, capable of detecting counterfeits, grey-market products, and tampering. We can also help implement secure marketing campaigns, by guaranteeing that only requests originating from authenticated tags are forwarded to your own web service. All other requests are blocked. In such cases, a defined action informs you and your customer about the failed request.

The advanced authentication engine is also available as stand-alone Authenticator for those who want to manage the tags themselves, but rely on NXP for enhanced security. NXP securely manages customer dedicated keys for its DNA and tamper evident products, and supports relevant cryptographic operations in a secure environment.

- Easy to use
- Flexible
- Scalable
- Multi-security
- Web-based interface to customer systems

€80

THREE WAYS TO A MORE ROBUST NFC SOLUTION

Our three NTAG cloud service offerings – **Validator & Redirector, Authenticator & Redirector, and Authenticator** – provide an optimized mix of features and work seamlessly across our broad selection of NFC chip products. The first two offers are full-service packages, including tag management, whilst the stand-alone Authenticator suits customers with their own tag management platform who in particular wish to rely on NXP's advanced security services.

NTAG VALIDATOR & REDIRECTOR

Tag management	Link individual tags or groups of tags to product URLs (hosted in customer's CMS) Links can be changed dynamically at any time
Infrastructure	Managed by NXP in cloud (on ntag.nxp.com)
Supported features	• Location and time awareness • Tap counter awareness • Originality signature validation • Blacklisting of suspicious tags
Response	Redirection to customer web page
Base analytics	Frequency, location, time, system & browser, fraudulent attempts
Supported products	NTAG 210 Micro, NTAG 213

This service can be used with pre-encoded NXP Standard Products. Alternatively, customers can select their own domain name and link their DNS entry to the NTAG Redirector.

Advantages:

- Faster time to market for product digitization
- Database with access to real-time and historical tag interactions
- Scalable, secure cloud infrastructure
- Risk management at scale and at low cost

NTAG AUTHENTICATOR & REDIRECTOR

Tag management	Link individual tags or groups of tags to product URLs (hosted in customer's CMS) Links can be changed dynamically at any time
Infrastructure	Managed by NXP in cloud (on ntag.nxp.com) Authentication supported by dedicated secure hardware (HSM)
Supported features	• Shared NXP master keys or dedicated customer keys to support cryptographic operations • SUN (Secure Unique NFC) message[1] and encrypted SUN message[2] verification to protect access to target URL • Die-individual tamper message verification to differ status response[3] • Mutual authentication to protect access to tag memory[4] • Blacklisting of suspicious tags
Response	Redirection to customer web page
Base analytics	Frequency, location, time, system & browser, fraudulent attempts
Supported products	NTAG 413 DNA[1,4], NTAG 424 DNA[1,2,4], NTAG 424 DNA TagTamper[1,2,3,4], NTAG 213 Tag Tamper[3]

This service can be used with pre-encoded NXP Standard Products. Alternatively, customers can select their own keys and domain name, and link their DNS entry to the NTAG Redirector.

Advantages:

- Faster time to market with secure end-to-end authentication solution
- Multi-security authentication solutions to meet your requirements

- Cost efficiency due to saved investment in server hardware and secure HSM equipment
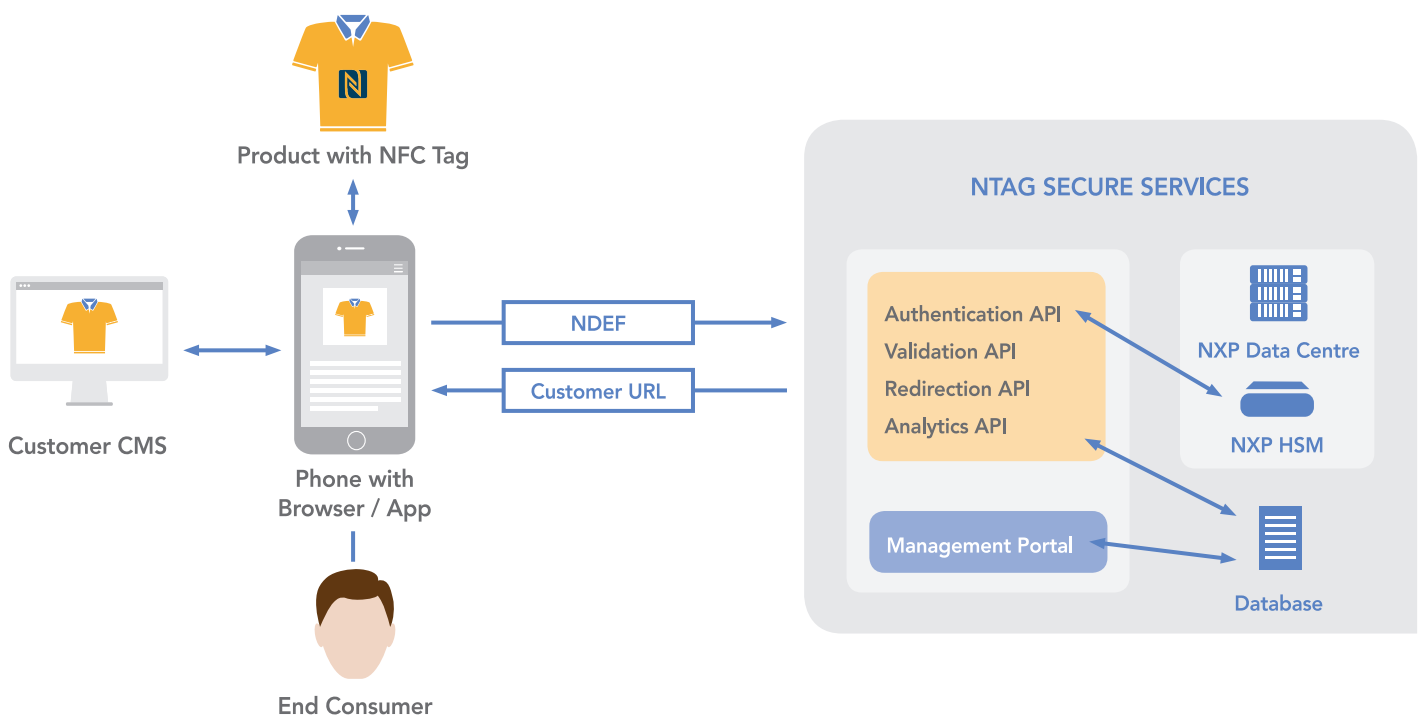- Flexible authentication APIs for mobile and web applications

NTAG AUTHENTICATOR

Infrastructure	Dedicated secure hardware (HSM) for key management to support cryptographic operation
Supported features	• Dedicated customer master keys for cryptographic operations • Secure key exchange • Secure key management
Response	Valid/invalid authentication request
Supported APIs for	• Secure Unique NFC (SUN) message[1] and encrypted SUN message[2] verification • Die-individual tamper message verification[3] • Mutual authentication[4]
Supported products	NTAG 413 DNA[1,4], NTAG 424 DNA[1,2,4], NTAG 424 DNA TagTamper[1,2,3,4], NTAG 213 Tag Tamper[3]

Available with NTAG Configure & Trust for customer URLs and dedicated secret keys.

Advantages:

- Multi-security authentication solutions meet your requirements
- Dedicated crypto keys for each customer

- Secure key management to minimize risk exposure and reduce your investment in hardware security (HSM)
- Flexible authentication APIs for mobile and web applications

Product with NFC Tag

Customer CMS

Phone with Browser / App

End Consumer

NDEF

Customer URL

NTAG SECURE SERVICES

Authentication API
Validation API
Redirection API
Analytics API

Management Portal

NXP Data Centre

NXP HSM

Database

Customer intelligence

Smart secured products come with better insights. IoT data supports businesses with real-time analytics, letting you know how products are performing, and detecting irregularities, so issues with authenticity, tampering, or grey markets can be dealt with immediately.

NTAG Secure Cloud Services collect data in real-time, provide ad-hoc reporting, and link seamlessly into your own business intelligence system, to help gather knowledge needed to make better decisions or take corrective actions.

Security and access

NTAG Secure Cloud Services adhere to state-of-the-art security standards and are regularly audited by NXP's Cybersecurity team. This includes a dedicated access control model based on 2-Factor Authentication (2FA) for backend access, logging of data requests and changes, and encryption of all critical data in transit and storage.

Authentication keys for tag ICs fitted with encryption are stored and managed only on dedicated secure hardware held within a state-of-the-art data center in Europe.

When needed, requests reaching your web server can also be protected, to ensure they originate from NXP's service.

Integration and support

NTAG Secure Cloud Services are accessible using standard RESTful APIs, to enable easy and fast integration into your cloud systems and software. Valuable support to help with the integration comes from our Customer Application Support team.

SECURE, FLEXIBLE, END-TO-END SOLUTIONS

NXP brings you complete NFC and IoT security solutions, offering end-to-end protection with best-in-class chip technology, trust provisioning, secure key management and advanced authentication services. Our solutions offer the most robust, multi-pronged product protection against counterfeiting and fraudulent attacks, while easing the integration into your existing platforms and applications.