

NFC 标签产品在不同行业的可追溯性应用

A Powerful Mix of Security, Privacy & Trust for NFC in today's IoT

Richard Qiu
NXP RFID & Security BD





溯源管理在IOT新商业模式中的重要性



溯源管理实现的必要条件



NXP DNA标签特性助力溯源管理实现



NXP NFC标签产品在溯源管理中的应用



技术支持资源和FAQ

□ 溯源重要性的思考

连接

In 2021, 1B+ additional consumers online

智能

In 2021, 40B+ intelligent products & devices



大数据

In 2021, 3.3T Gbyte of IP traffic

□ 溯源管理是物联网模式的最佳基础和实践



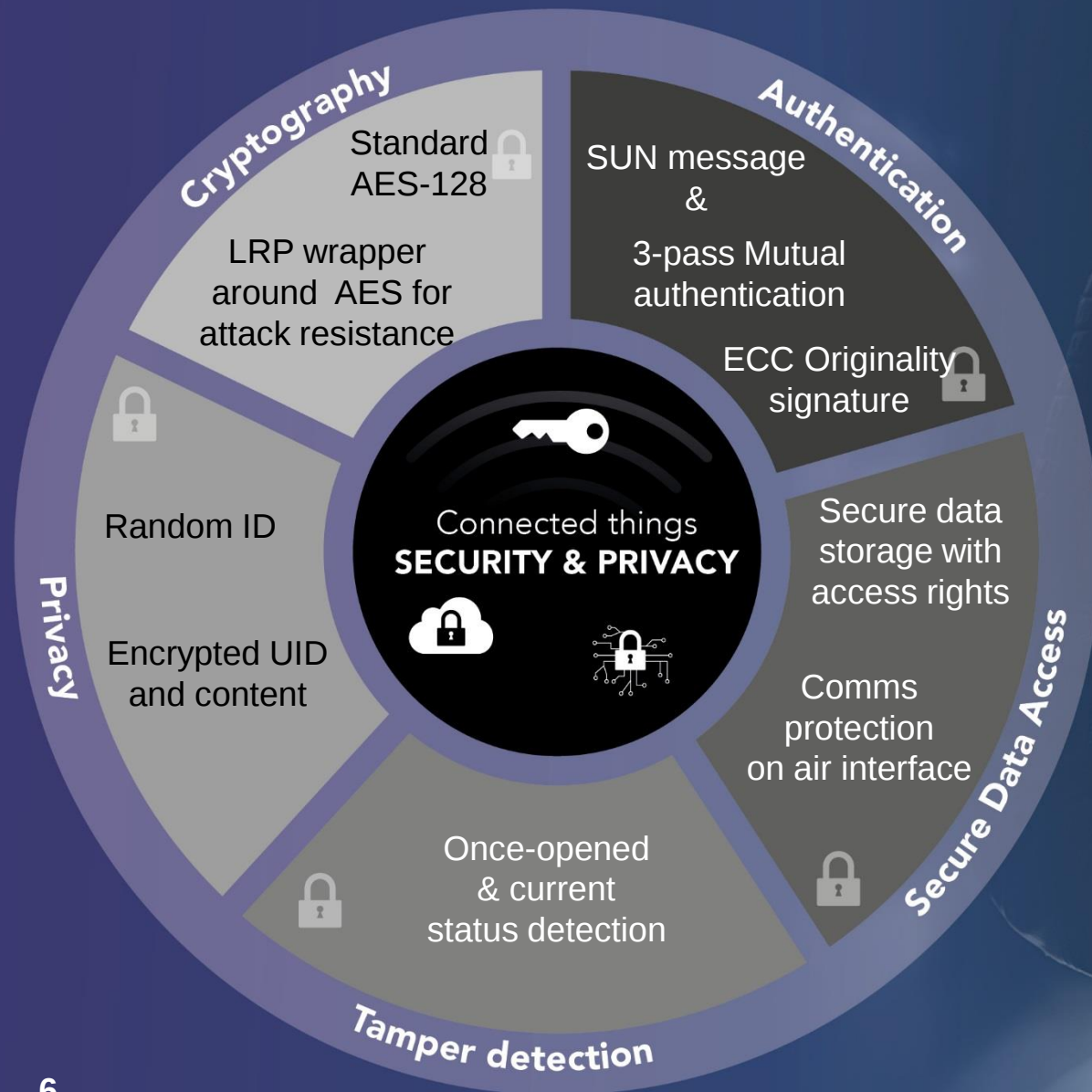
□ 实现必要条件的基础



□ NXP DNA 系列产品助力溯源



□ NTAG 424 DNA TagTamper 特性



NFC Forum Type 4 Tag,
ISO14443-A compliant

CC EAL 4 targeted for
Hardware and Software

Comms speed up to 848
kbit/s
Benchmark performance



COMMON CRITERIA
CERTIFICATION
TARGETED

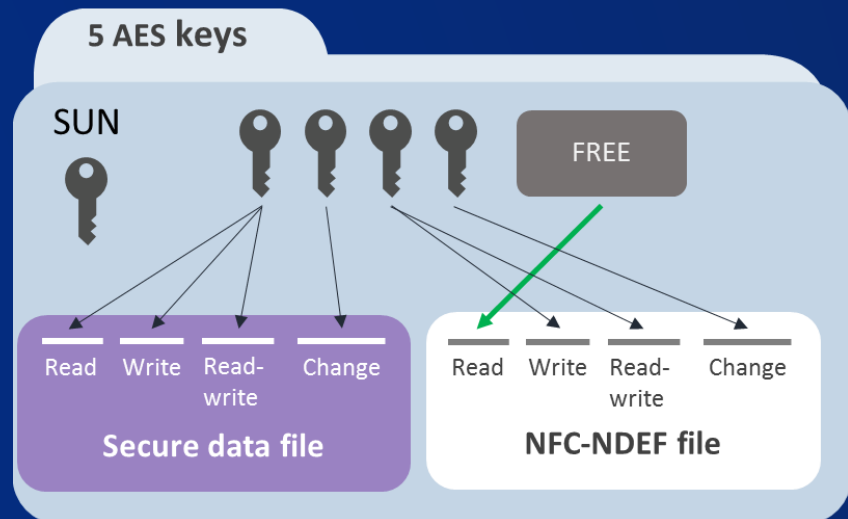
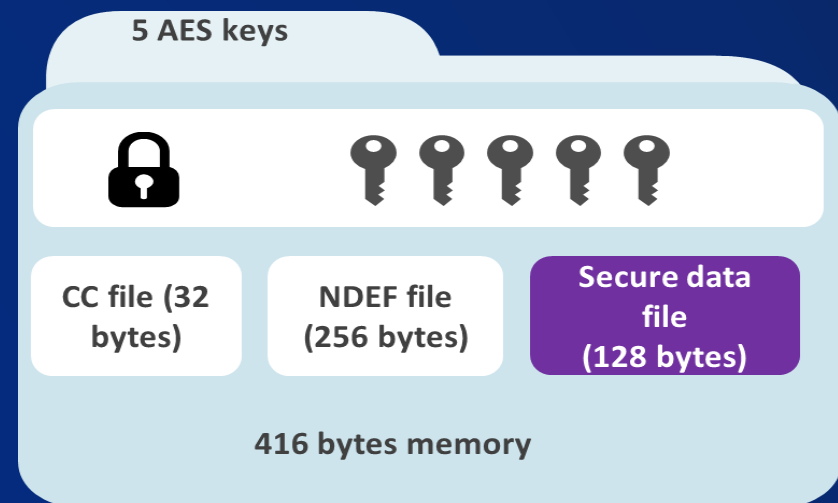


➤ 416 bytes 存储空间, 3 个标准数据文件

- ISO-IEC 7816-4 文件系统
- CC file, NDEF file, secure data file

➤ 5 个可配置AES密钥, 用于满足个性化访问安全的需求

- SUN NDEF 信息加解密
- 用于安全访问的相互认证
- 加密通讯, 可满足隐秘访问



➤ 软硬件通过CC EAL 4+ 安全等级认证,提供EAL5+ 金融级密钥和数据注入服务

Name	Title
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers
T.Masquerade_TOE	Masquerade the TOE

Tab. 3.1: Threats defined in the Protection Profile

Difficult to probe,
and detect if there is probe

Good random numbers

Always work as intended

Name	Title
T.Data-Modification	Unauthorised Data Modification
T.Impersonate	Impersonating authorised users during authentication
T.Cloning	Cloning

Tab. 3.2: Additional Threats defined in this Security Target

No data modification

No cloning

□ 从标签到云 构建安全的IoT实例

- 产品和IoT平台**安全连接**, 防止数据复制,篡改和破坏
- **优秀的品牌保护能力**,对抗伪造和灰色市场
- **安全的动态数据**, 保证数据安全,真实且唯一,不惧公开



SECURE ELEMENT
in an **NFC TAG**



□ SUN 让每一次触碰都是唯一



- SUN 为每一次数据读取进行加密, 且可以被任何标准 NFC 手机访问
- 和云端服务器进行安全的直接认证和数据交换

<https://www.brand.com/.../>

UID + Content
encryption

CMAC code

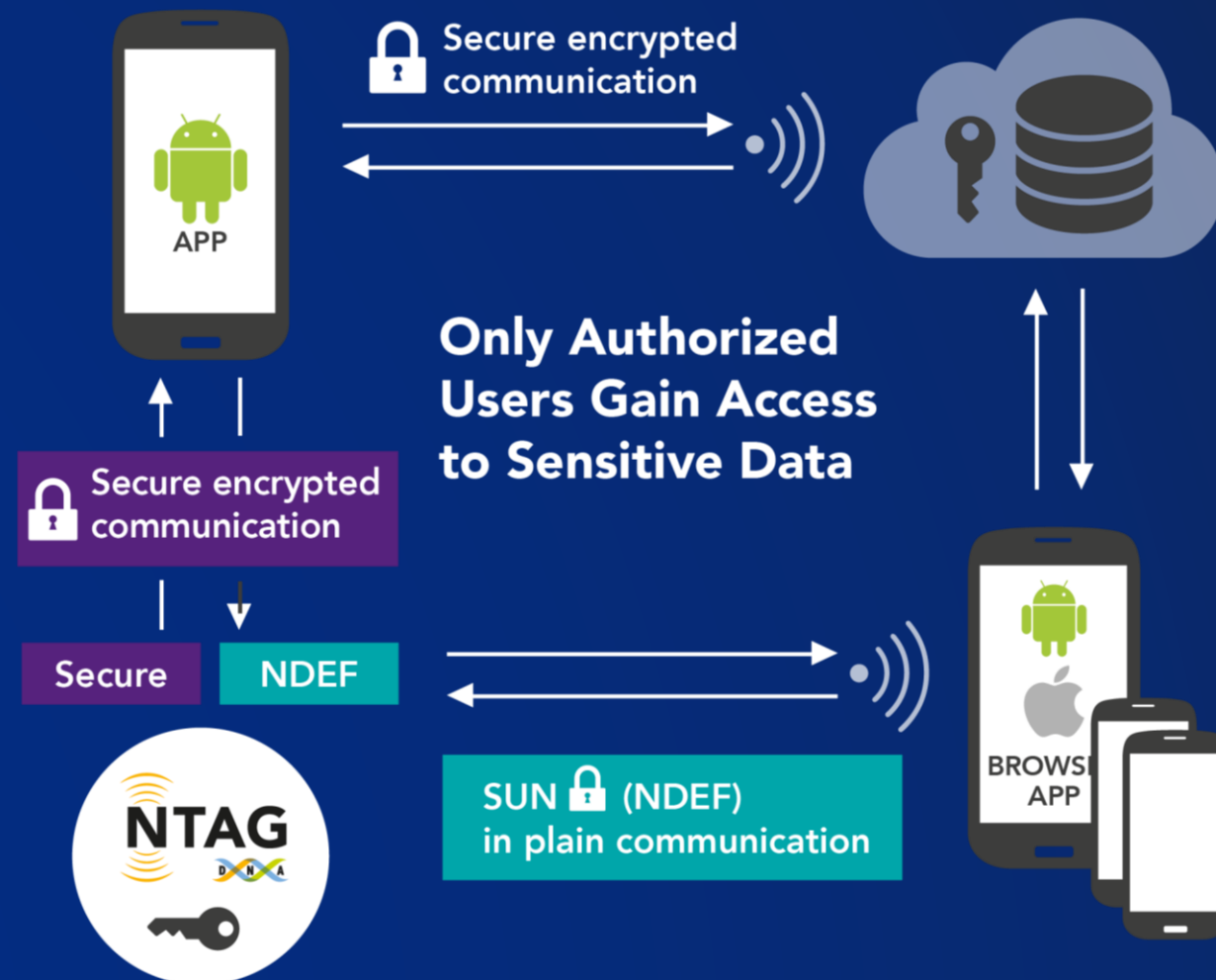
SUN

UID / Tap counter /
Tamper status

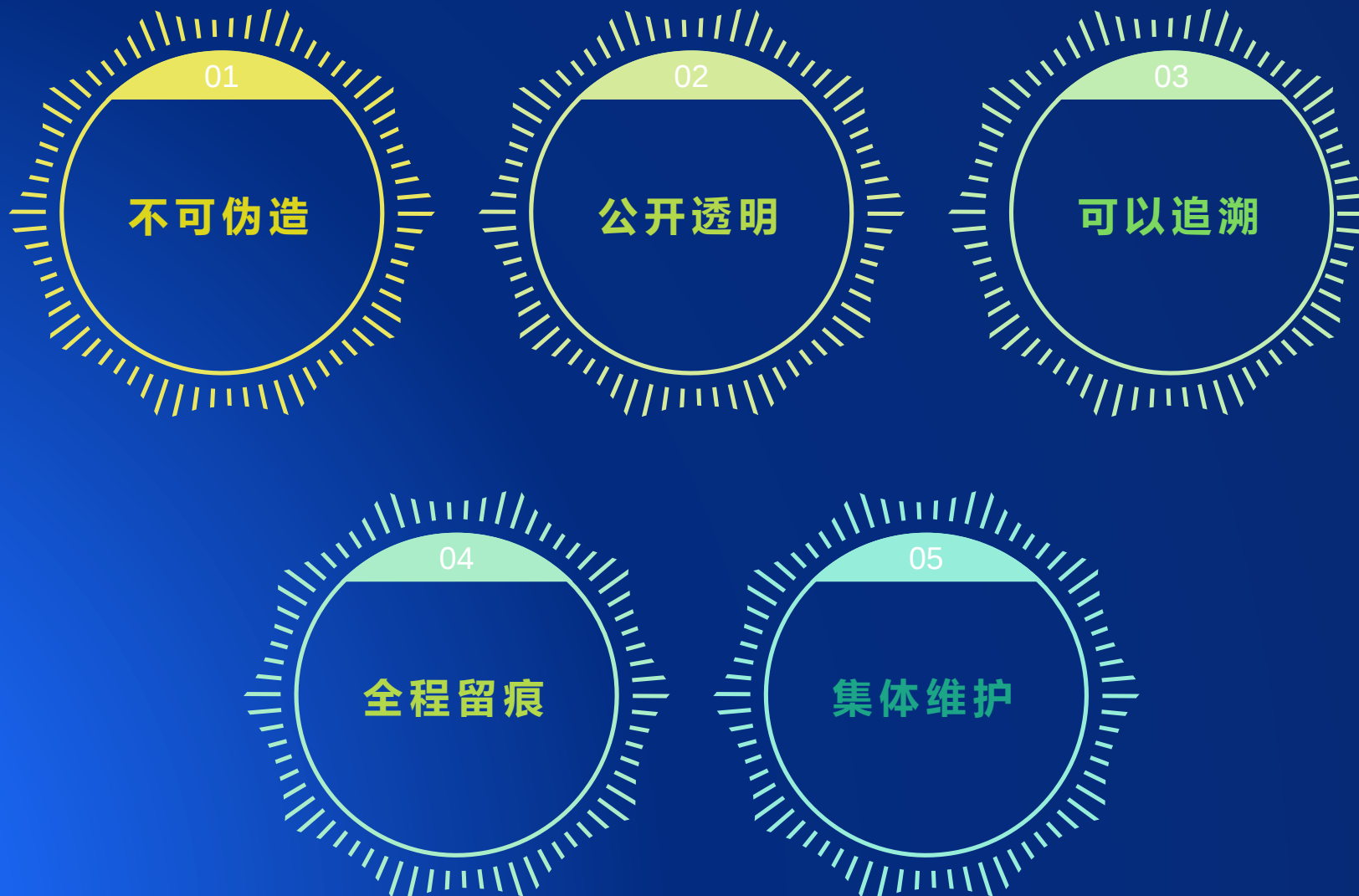
URI + cryptogram

□ SUN vs 隐私数据存储

- SUN 数据通过透明模式传递,支持标准NFC手机读取, 无须特殊APP支持
- 特殊用户可经过加密交互认证访问隐私数据区, 数据传输全程保持加密,可防止边际侦测破解



□ 溯源体系实现的必要条件



□ UCODE DNA 特性

privacy
高精细化隐私数据保护

High Speed
无与伦比的高速读写认证体验

Long Range

世界领先的UHF 无线性能

Security

世界领先的标签级安全认证算法实现



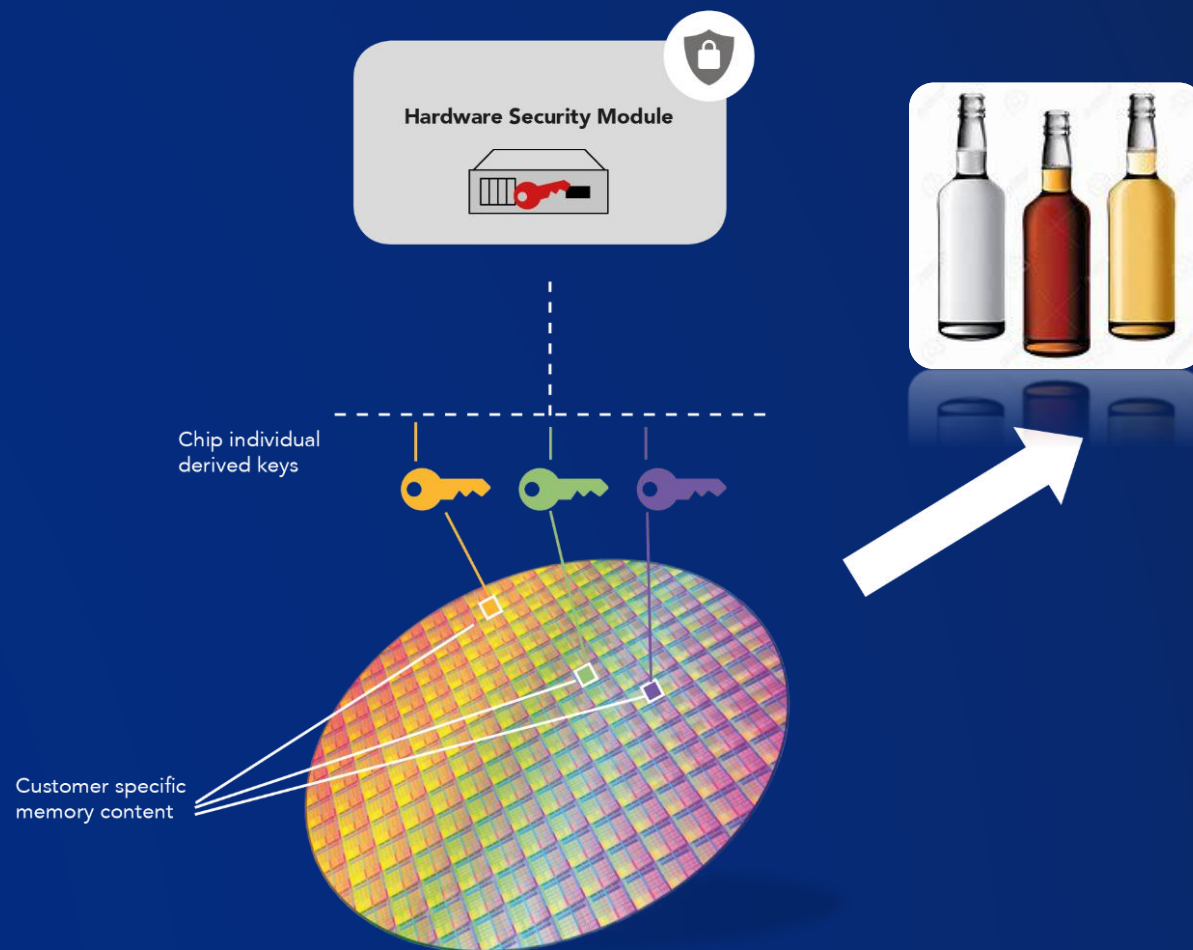
□ 提供金融安全级的晶圆密钥数据注入服务

➤ NXP Trust Provisioning

- 提供晶圆级AES密钥生成和分散服务,提供金融认证的EAL5+密钥管理环境
- 在NXP EAL5+安全工厂进行密钥分散,并将密钥数据注入每一个晶圆

➤ NXP Encoding

- 根据客户提供的特殊数据规范,进行超高速的IC 数据编程和烧入



□ NFC 让IOT进入日常生活



NFC phone
to connect to cloud

Product ID management,
Real-time data management,
Analytics



Social platforms



Consumer
& business mobile apps



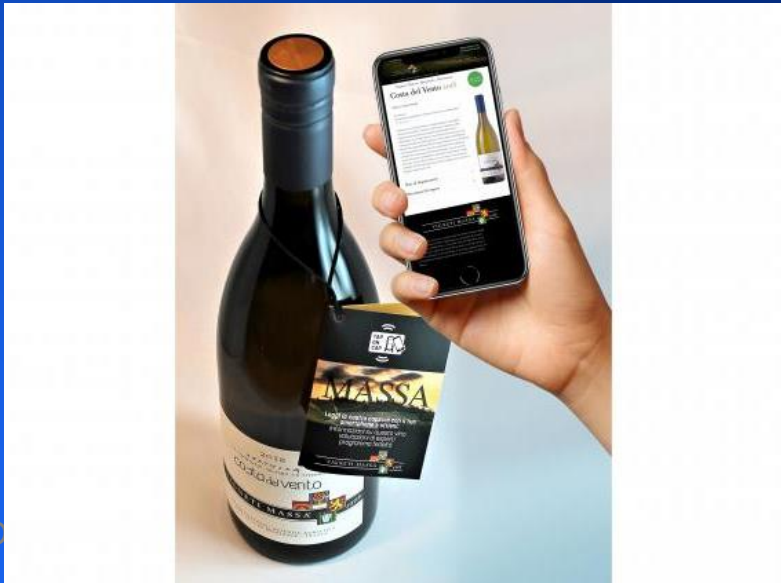
BI & CMS systems



Enterprise
& Supply chain systems



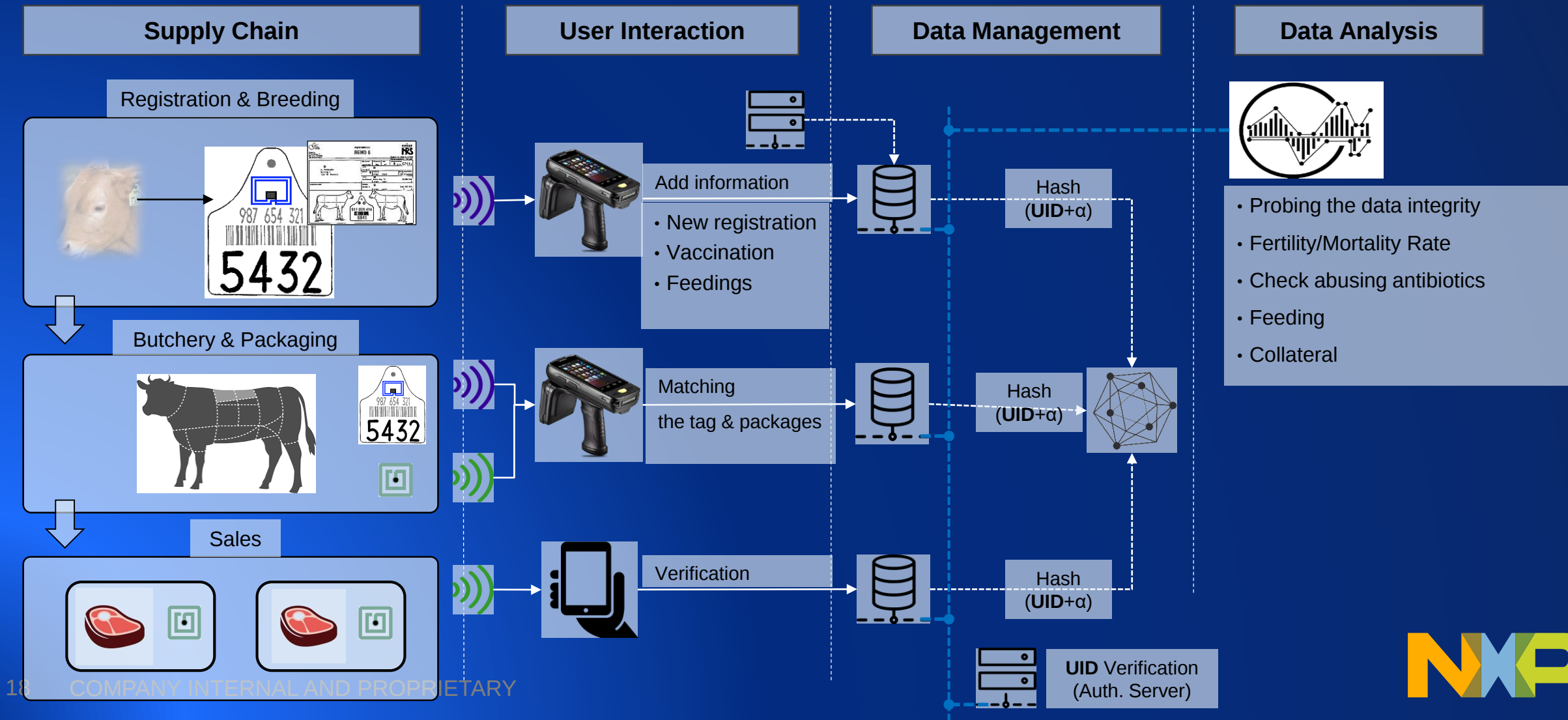
□ 案例一



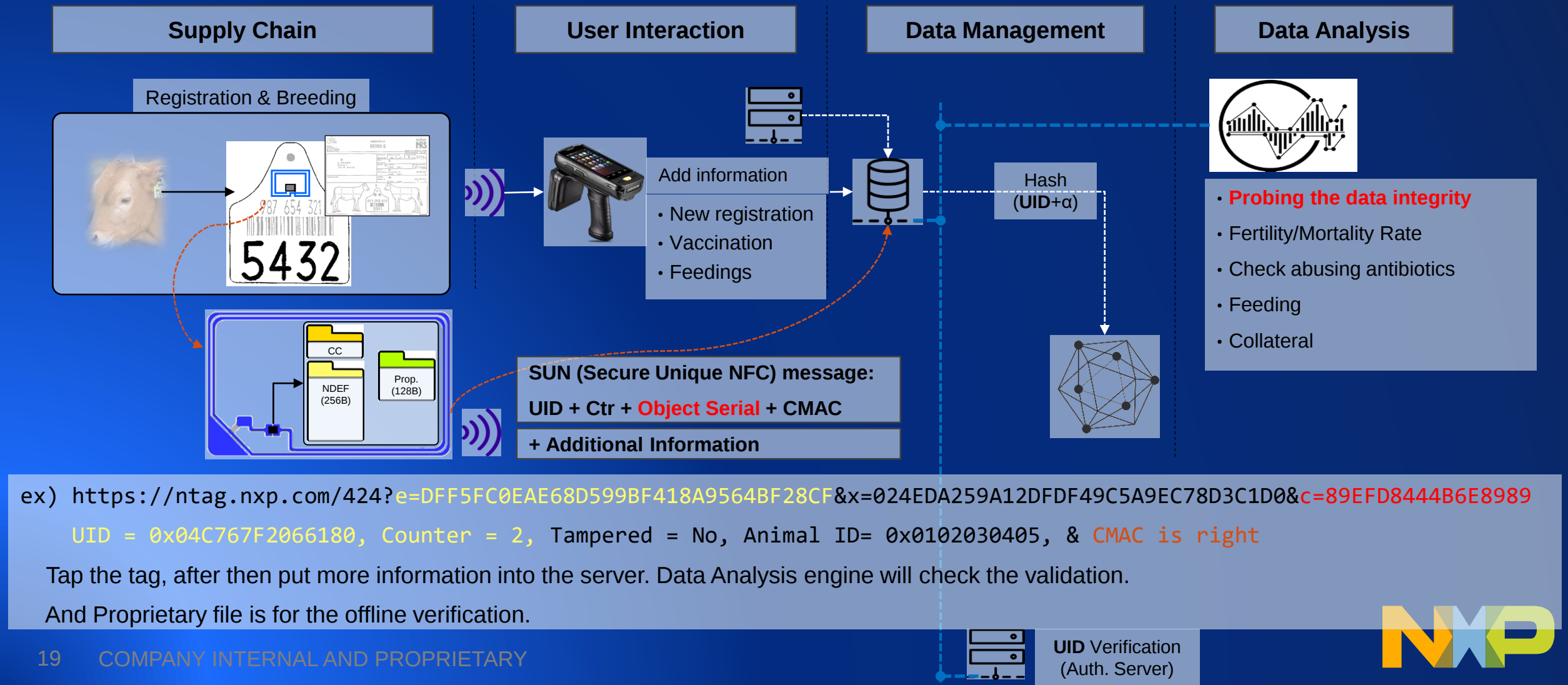
□ 案例二



NTAG + UCODE溯源案例



□ NTAG + UCODE 溯源案例



❑ Overview of available NXP services offering

	Entry level ICs			Advanced ICs		
	NTAG 210 micro	NTAG 213	UCODE 8	NTAG 213 Tag Tamper	NTAG 4xx DNA	UCODE DNA
Encoding	✓	✓	✓	✓	✓	✓
Trust Provisioning	✗	✗	✗	✓	✓	✓
Validation & Redirection	✓	✓	✗	✗	✗	✗
Authentication & Redirection	✗	✗	✗	✓	✓	✗
Standalone Authentication	✗	✗	✓	✓	✓	✓

Q&A

Thank You