Best practices for security and privacy with ST25 NFC/RFID tags

Introduction

Every NFC/RFID system includes a radio frequency (RF) subsystem, composed of tags and readers, such as a smartphone. The RF subsystem is supported by middleware, analytic systems, and networking services. Each NFC/RFID ecosystem has different components and customizations and, as a result, the security risks and the controls available to address them can be fairly different.

This document details the available security and privacy countermeasure controls available when using the products listed in Table 1. The provided guidelines focus on available controls, such as deterrence, prevention, detection, and recovery, at any layer of this ecosystem. The document does not address the advanced authentication and cryptography features of the RF subsystem that can be incorporated into secure ST devices with NFC/RFID capabilities.

Table 1. **Applicable products**

Product class	Product series or RPN
ST25 NFC/RFID tags and readers	ST25DV-I2C and ST25DV-PWM series dynamic NFC tags
	ST25TB, ST25TN, and ST25TV series NFC tags
	ST25TA02KB, ST25TA02KB-D, ST25TA02KB-P, ST25TA16K, ST25TA64K

1 Overview

1.1 Intended audience

NFC/RFID technology can help a wide range of organizations and individuals achieve significant gains in productivity and efficiency.

Like any information technology (IT), radio frequency identification (RFID) carries security and privacy risks that must be mitigated through management, operational and technical controls, to exploit its benefits.

These organizations and individuals include hospitals and patients, retailers and customers, manufacturers and distributors throughout the supply chain, as well as other organizations that offer a wide range of solutions covering many applications in everyday life.

1.2 Document structure

This application note provides an overview of the ST25 NFC / RFID Tags listed in Table 1. Applicable products, their associated security and privacy risks and responses, and recommended practices. These enable any organization to realize productivity improvements while safeguarding sensitive information and protecting the privacy of individuals.

The document is organized in three sections:

- Section 3: NFC/RFID technology and applications presents the NFC / RFID ecosystem with the risks to be addressed, and identifies application requirements in terms of security and privacy among the most popular NFC / RFID applications.
- Section 4: NFC/RFID risks describes the threats and associated risks in terms of security and privacy.
- Section 5: Security controls explains the various NFC / RFID security controls that can be deployed with the ST25 NFC / RFID Tags. This includes their benefits, limitations, and recommendations that organizations using these products can follow throughout the system life cycle.

Note: *ST25 NFC /RFID Tags devices are not certified products that can be used in entry level security applications. In case of needs of a more secure solution as in the transportation domain, for example, STMicroelectronics can propose the CD21 product portfolio using the certified secure ST31 IC family and compliant with all Calypso requirements.*

2 General information

2.1 Acronyms and abbreviations

Table 2. **Acronyms used in this document**

Acronym	Definition
CRC	Cyclic redundancy check
DoS	Denial of service
EAS	Electronic article surveillance
EEPROM	Electrically-erasable programmable read-only memory
HMAC	Keyed-hash message authentication code
ISO	International Organization for Standardization
ID	Identifier
IEC	International Electrotechnical Commission
IT	Information technology
GDPR	General data protection regulation
NFC	Near-field communication
OTP	One-time programmable
PKI	Public-key infrastructure
RF	Radio frequency
RFID	Radio-frequency identification
R+T	Reader plus tag strategy
SNMP	Simple network-management protocol
TD	Tamper detection
UID	Unique identifier
URL	Uniform resource locator
WORM	Write once, read many

2.2 Glossary

Table 3. **Glossary of terms**

Term	Definition
Analytic systems	IT systems that process the information outputs produced by middleware. Analytic systems may be comprised of databases, data processing software, and Web services.
Back channel	The channel on which a tag transmits its signals.
Backscatter channel	The type of back channel used by passive tags.
Brute-force attack	Method to gain access to the tag memory with trials of various combinations of passwords again and again until it gets in.
Cloned tag	A tag that is made to be a duplicate of a legitimate tag.
Cover-coding	A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted.
Duty cycle	The percentage of time that the device is emitting energy over a specified period.
Denial of service	A party seeks to make a device or network resource unavailable to its intended users by temporarily or indefinitely disrupting services.
Dynamic tag	A tag that relies on a battery for power when needed.
Eavesdropping	A party that secretly receives communications intended for others.
Enterprise system	The portion of the RFID system that analyzes, processes, and stores information collected by the RF subsystem. An enterprise subsystem is made up of middleware, analytic systems, and network infrastructure.
Form factor	The physical characteristics of a device or object, including its size, shape, packaging, handling, and weight.
Forward channel	The channel on which a reader transmits its signals.
Forward channel eavesdropping range	The distance over which a rogue receiver can reliably listen to the transmissions of an authorized reader.
Jamming	Deliberate communications disruption, achieved by interjecting electromagnetic waves on the same frequency as that used by the tag reader.
Middleware	Software that aggregates and filters data collected by RFID readers and possibly passes the information to an enterprise subsystem database.
Passive tag	A tag that does not have its own power supply. Instead, it uses RF energy from the reader for power.
Reader	A device that can wirelessly communicate with tags.
Reader spoofing	The act of impersonating a legitimate reader of an RFID system to read tags
RF subsystem	The portion of the RFID system that uses radio frequencies to perform identification and related transactions.
Rogue skimming (or scanning) range	The distance over which a rogue reader operating above regulated power limits can reliably communicate with a tag.
Skimming	The unauthorized use of a reader to read tags without the authorization or knowledge of the tag’s owner, or the individual in possession of the tag.
Spoofing	An adversary impersonates a valid tag to gain its privileges. This impersonation requires full access to the same communication channels as the original tag.
Tamper resistance	A technique to eliminate the risks of brute-force attack by increasing the password length.

2.3 Reference documents

The documents listed in Table 4 are available on request through ST technical support.

Table 4. Reference documents

Reference	Document
[1]	AN5101 - TruST25™ digital signature for ST25TA512B, ST25TA02KB, ST25TA02KB-D and ST25TA02KB-P devices, application note (ST Restricted document).
[2]	AN5103 – Password encryption for ST25TV512 and ST25TV02K devices, application note (ST Restricted document).
[3]	AN5104 - TruST25™ digital signature for ST25TV512 and ST25TV02K devices, application note (ST Restricted document).
[4]	AN5262 – How to manage simultaneous I²C and RF data transfer with an ST25DVxxK device, application note (ST Restricted document).
[5]	AN5323 - ST25DV-I2C crypto demonstration, application note.
[6]	AN5364 - How to protect ST25 tags from wireless power charging, application note.
[7]	AN5149 - TruST25™ digital signature for ST25DV02K-W1, ST25DV02K-W2 devices, application note (ST Restricted document).
[8]	AN5439 - Augmented NDEF with ST25DV-I2C series Dynamic NFC Tags, application note.
[9]	AN5580 - TruST25 digital signature for ST25TV512C and ST25TV02KC devices, application note (ST Restricted document).
[10]	AN5624 - How to manage simultaneous I²C and RF data transfer with an ST25DVxxKC device, application note.
[11]	AN5658 - Augmented NDEF messages with ST25TV512C and ST25TV02KC devices, application note.
[12]	AN5660 - TruST25 digital signature for ST25TN512 and ST25TN01K devices, application note (ST Restricted document).
[13]	AN5680 - Augmented NDEF messages with ST25TN512 and ST25TN01K devices, application note.
[14]	DS10925 - Dynamic NFC/RFID tag IC with 4-, 16-, or 64-Kbit EEPROM, and fast transfer mode capability, datasheet.
[15]	DS11364 - 13.56 MHz short-range contactless memory chip with 4096-bit EEPROM and anticollision functions, datasheet.
[16]	DS11456 - 13.56 MHz short-range contactless memory chip with 512-bit EEPROM and anticollision functions, datasheet.
[17]	DS11469 - 13.56 MHz short-range contactless memory chip with 2048-bit EEPROM and anticollision functions, datasheet.
[18]	DS11495 - 13.56 MHz short-range contactless memory chip with 512-bit EEPROM and anticollision functions, datasheet.
[19]	DS12074 - NFC Type 5 / RFID tag IC with up to 2-Kbit EEPROM, product identification and protection, datasheet.
[20]	DS12114 - Dynamic NFC/RFID tag IC with up to two PWM outputs and 2-Kbit EEPROM, datasheet.
[21]	DS12365 - NFC Forum Type 4 Tag IC with up to 2-Kbit EEPROM, datasheet.
[22]	DS13304 - NFC Type 5 / RFID tag IC with up to 2.5 Kbits of EEPROM, product identification and protection, datasheet.
[23]	DS13433 - NFC Forum Type 2 tag IC with up to 1.6 Kbits of EEPROM, datasheet.
[24]	DS13519 - Dynamic NFC/RFID tag IC with 4-Kbit, 16-Kbit or 64-Kbit EEPROM, fast transfer mode capability and optimized I2C, datasheet.

3 NFC/RFID technology and applications

Various applications use different combinations of components and have different sets of risks. An application may determine the location of goods attached to tags, or their presence and possibly their authentication. Another application might only need a unique static identifier value for each tagged object, while others may need to store additional sensitive information about each tagged object over time.

The physical and technical environment should also be considered at the time an NFC/RFID tap occurs, but also before and after it. This includes the distance between the reader and the tag, the time interval in which each tap must be performed, and the threats that might occur while the tagged objects are in storage and transit.

Organizations need to assess the risks they face and choose appropriate technical security controls for their environments. These assessments should take many factors into account, such as application or regulatory requirements. Privacy regulations and guidance, for example, are often complex and change over time.

To be most effective, NFC/RFID security controls should be incorporated throughout the entire life cycle of the products.

3.1 RF subsystem

To enable wireless identification, the RF subsystem uses two components:

- **NFC/RFID tags**. These are small electronic devices stuck to objects or embedded in them. Each tag has a unique identifier and other features, such as memory to store additional data and security mechanisms. STMicroelectronics guarantees the uniqueness of UID for each delivered device.
- **NFC/RFID readers**. These are devices that wirelessly communicate with tags to identify the item connected to each tag.

Figure 1. **Types of RF subsystem**

Section 3.1.1: Main tag characteristics provides information to help organizations using NFC/RFID systems to identify the tag characteristics required in their environment and applications.

3.1.1 Main tag characteristics

3.1.1.1 *Performance*

These characteristics include operating range, speed of reads, and RFID data transfer rate. In general, as the operating frequency increases, it is possible to exchange more data. As a result, higher frequency readers are also able to read more tags in a given period of time.

Table 5. **ST25 performance characteristics**

Series	ST25TA	ST25TB	ST25TN	ST25TV	ST25DV-I2C	ST25DV-PWM
Frequency	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz
Operating range[1]	< 7 cm	< 7 cm	< 7 cm	< 75 cm	< 75 cm	< 75 cm
Data rate	106 kbps	106 kbps	106 kbps	Up to 53 kbps[2]	Up to 53 kbps	26.5 kbps

1. *Values when specific conditions are met.*
2. *ST25TV series only. Up to 23 kbps for the ST25TVKC series.*

For most applications, increased speed and operating range are considered advantageous. An exception is applications for which security or privacy is a significant concern. For these, the ability of an adversary to read the data more quickly and from a longer distance is typically considered to be a risk that requires mitigation.

Tag performance characteristics also include the ability of the tag's signal to penetrate materials. Depending on the application, the penetration capabilities of a particular frequency can be either a benefit or a shortcoming. For applications in which security is a significant concern, an organization may use a frequency range that can be blocked by a particular material because this enables effective security shielding, which might not otherwise be available.

Table 6 shows the ability of RF signals to penetrate various substances embedding ST25 NFC/RFID tags.

Table 6. **ST25 NFC/RFID tag physical characteristics**

Material	Tag property
Clothing	Transparent
Dry wood	Transparent
Graphite	Transparent
Metal	Opaque
Motor oil	Transparent
Paper products	Transparent
Plastics	Transparent
Water	Transparent
Wet wood	Transparent

3.1.1.2 *Tag functionality*

The primary function of a tag is to provide an identifier to a reader, but many types of ST tags support additional capabilities that are valuable for certain business processes. These include:

- **Memory (non-volatile)**. This enables data to be stored on tags and retrieved at a later time. This memory is either write once, read many (WORM) memory or re-writable memory, which can be modified after initialization.
- **Security functionality** . In the resource-constrained environment, tags with on-board memory are often coupled with security mechanisms to protect the stored data. For example, some tags support mechanisms that can prevent further modification of data in the tag memory, prevent access to data in the tag memory, or ensure more secure RF transmission. Some tags also offer tamper protection as a physical security feature.

- **Privacy protection mechanisms**. Privacy-related threats, including tracking, data linking, behavioral profiling and host listing are covered by proprietary mechanisms. The ST25 NFC / RFID Tag does not prevent the privacy-related threats but assists customers to mitigate the privacy-related threats with its privacy protections. The privacy capabilities offer some specific mechanisms, such as pseudonymization, programmable and optional concatenation concerning tag assets, anonymity, obfuscation, and encryption. However these are not the only privacy protection mechanisms that can be embedded into the tags.

The major ST25Tx series device security and privacy functionalities are summarized in Table 7.

Table 7. **ST25Tx series controls**

Countermeasures	ST25TV	ST25TA	ST25TB	ST25TN
Password authentication	Supported	Supported	-	-
Permanent access control	Supported	Supported	Supported	Supported
Temporary access control	Supported	Supported	-	-
ID chip selection	Supported	Supported	Supported	Supported
Temporary deactivation	Supported	-	-	-
Kill	Supported	-	-	Supported
Digital Signature	Supported	Supported	-	Supported
Tamper resistance	Supported	Supported	-	-
Cover coding	Supported	-	-	-
Anti-tearing	Supported	Supported	Supported	Supported
Seal integrity	Supported	-	-	-
Data encryption in transit	-	-	-	-
Cloud-based authentication	Supported(1)	-	-	Supported

1. Only supported by ST25TV512C and ST25TV512KC.

The major ST25DV-xxx device security and privacy functionalities are summarized in Table 8.

Table 8. **ST25DV-xxx series controls**

Countermeasures	ST25DV-I2C	ST25DV-PWM
Password authentication	Supported	Supported
Permanent access control	-	Supported
Temporary access control	Supported	Supported
ID chip selection	Supported	Supported
Temporary deactivation	Supported	-
Kill	-	-
Digital signature	-	Supported
Tamper resistance	Supported	Supported
Cover coding	-	-
Anti-tearing	-	-
Seal integrity	-	-
Data encryption in transit	Supported	-
Cloud-based authentication	Supported	-

3.1.1.3 *Form factor*

The form factor of a tag refers to its shape, size, packaging, and handling features. Important aspects of tag form-factor include the size of the tag, its weight, and the method by which the tag is affixed to and removed from its associated object. Tags can be attached to items using an adhesive or can be embedded within the item. The primary concern when a tag is attached to an item is how easily it can be detached, whether accidentally or maliciously. Tags attached to items also are more vulnerable to harsh environmental conditions such as dust, debris, humidity, precipitation, and extreme temperatures.

Tags that are embedded in objects are less vulnerable to tampering and environmental conditions.

3.1.2 Main reader characteristics

To communicate, the tag and the reader must comply with the same standard.

Note: *ST offers complete R+T solutions, based on a reader and a tag. This prevents inter-device compliance issues for proprietary features.*

3.1.2.1 *Power output and duty cycle*

In most cases, standards and regulations determine the permitted power output and duty cycle of the readers. Readers that communicate with passive tags need greater power output than those that communicate with active tags, because the signal must be strong enough to reach the tag and enable the backscatter to return to the reader. In general, readers with greater power output and duty cycles can read tags more accurately, more quickly, and from longer distances. However, the greater power output also increases the risk of eavesdropping.

3.1.2.2 *Antenna design and placement*

Readers use a wide variety of antenna types. Each type has a different coverage pattern. To reduce the likelihood of eavesdropping and minimize interference with other radios, the coverage should only encompass a range sufficient to communicate with the intended tags. Antennas may be integrated into the device or may be detachable. Readers that support detachable antennas are better suited for applications that require specific coverage areas, because an antenna can be selected or customized to meet those requirements.

3.1.2.3 *Tag-reader communication*

Tag-reader communication uses a common communications protocol between the tag and the reader. Tag-reader communication protocols are often specified in RFID standards. The communications link between a tag and a reader is typically bi-directional. The reader transmits a signal to a tag over the *forward channel*. The tag responds on the *back channel*, which is also called the *reverse channel* or *backscatter channel*. When RFID systems use passive tags, signals on the forward channel are typically much more powerful than those on the back channel. Therefore, signals on the forward channel can be detected or properly received over longer distances. This difference has important implications for RFID communications security, including both the vulnerability of RF subsystem traffic and the mechanisms used to protect it.

3.1.2.4 *Eavesdropping range*

Eavesdropping range can be significantly greater than the nominal operating ranges listed in Table 5. For example, ISO/IEC 14443 tags have a typical operating range of around 10 cm. However, security researchers have used a portable, low-power device to demonstrate that the scanning range of an ISO/IEC 14443 contactless smartcard is at least 25 cm. Attacks exploiting rogue-scanning or forward channel eavesdropping ranges, are not possible for the sensitive commands of some ST25 NFC/RFID tags, because the mandatory cover-coding requires the reader to receive a password from the tag before issuing a command or a feature. Cover-coding is a technique used to obscure the content of messages from reader to tag.

The mechanisms and protections implemented in ST25 NFC/RFID tags are described in detail in Section 5.

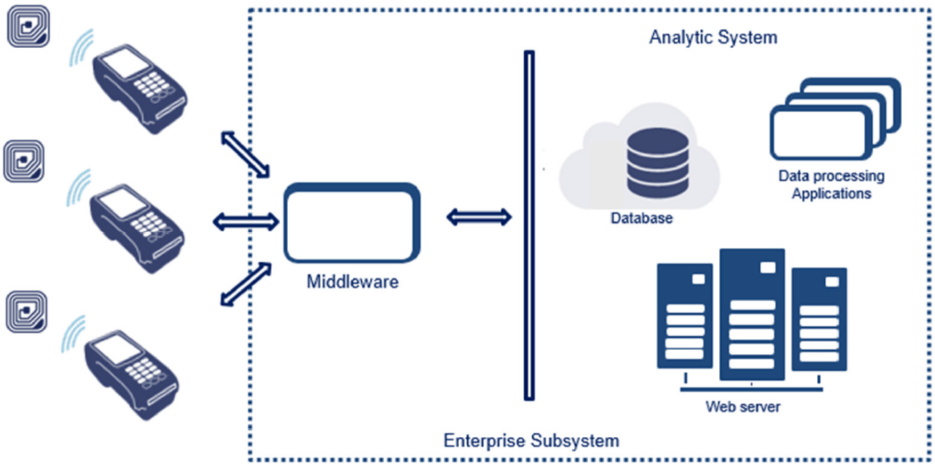
3.1.2.5 *Enterprise-subsystem interface*

Most readers have a second interface (in addition to that used to communicate with tags), to communicate with the enterprise subsystem (see Figure 2. Enterprise subsystem). The enterprise-subsystem interface supports transfer of RFID data from the reader to enterprise subsystem computers for processing and analysis. In most cases, the enterprise subsystem interface is used for remote management of the readers. The interface may be a wired (for example Ethernet) or wireless (for example Wi-Fi or satellite) link. The enterprise subsystem involves common IT components such as servers, databases, and network, and can therefore benefit from typical IT security protocols (SNMPs) for the links, and controls for the components

3.2 Enterprise subsystem

The enterprise subsystem connects readers to computers running software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful for a supported business process. The upper layers, composed of server, database or network services, can benefit from typical IT security controls for those components. Some simple RFID systems consist of an RF subsystem only (RFID systems in which a reader can make an access control decision without access to other computers). However, most RFID systems have both RF and enterprise subsystems.

Figure 2. **Enterprise subsystem**



The enterprise subsystem consists of the following three main components:

- **RFID middleware**. This is responsible for preparing data collected from readers in the RF subsystem for the analytic systems that directly support business processes. Middleware hides the complexity and implementation details of the RF subsystem from the analytic systems. Middleware filters are present to duplicate incomplete and erroneous information received from readers. Middleware filtering is especially useful for applications in which large numbers of tags are in close proximity. The middleware can immediately transfer the filtered data to the analytic systems or aggregate and store it for later retrieval.
- **Analytic systems**. These are composed of databases, data processing applications and Web servers that process the data outputs of middleware based on business requirements and user instructions. They contain customized business logic for each business process they support. Analytic systems correlate RFID data with non-RFID business records imported from other databases, such as records from business partners, customers, logistics service providers and suppliers. Correlation between RFID data coming from one single RFID device is also recommended in analytic systems for some applications: passive tags with primary and unitary services do not prevent spoofing of legitimate readers and communicate with any readers without detection or deterrence control when RFID data, stored in the RFID device, are inconsistent.
- **Network infrastructure**. This enables communication between the RF and enterprise subsystems, as well as among components of the enterprise subsystem. The physical topology of a network infrastructure supporting an RFID system depends on the physical location of the components in its enterprise subsystem:
  - If RFID transactions are relatively infrequent, the middleware can be placed in a central location to serve multiple readers.
  - If the business process requires large numbers of tags to be read quickly (for example multiple checkout stations in a busy store), the middleware is located near the readers to avoid latency problems and data throughput restrictions associated with many wide-area networks.

The physical location of analytic systems usually depends on how an organization manages its enterprise applications:

- If the analytic systems are dedicated to the RFID application, organizations often place these systems near readers and middleware.
- Some organizations locate their analytic systems in remote data centers to take advantage of the centers' physical security.

- If the analytic systems integrate both RFID and non-RFID information systems, it is unlikely that the location of the RF subsystem significantly influences the location of the analytic systems.

Data communications protocols are a critical component of a network’s performance, reliability, and security:

- The most common link-layer protocol connecting RFID enterprise subsystem components is Ethernet (IEEE 802.3). Ethernet has no built-in security functionality, which means other complementary data communications protocols must provide any required protection.
- In most RFID implementations, data communication within the enterprise subsystem is wired communication. The exception is mobile readers, which connect to the enterprise subsystem using a wireless link-layer protocol, such as Wi-Fi (IEEE 802.11). Wi-Fi characteristics are significantly different; Wi-Fi equipment supporting Wi-Fi Protected Access (WPA) includes numerous security features, such as strong authentication and encryption.

3.3 NFC/RFID applications and requirements

Applications for RFID technologies are diverse due to their use in a wide range of business processes. RFID security risks and the controls available to mitigate them are also highly varied.

There are many types of RFID application, their key differentiating characteristic being the purpose for which the tagged items are identified.

Table 9. **Example applications**

Purpose and identification	Application type
Determine the presence of an item	Asset management
Determine the location of an item	Tracking
Determine the origin of an item	Authenticity verification
Correlate information with the item for decision-making	Process control
Authenticate access privileges	Access control

The user must understand which implementations apply to its application, to select appropriate security controls, and be aware that counterfeiters may leverage RFID technology for unintended purposes.

3.3.1 NFC/RFID applications

3.3.1.1 Asset management

RFID-based asset management systems are used to manage inventory of any item that can be tagged. Perhaps the simplest form of asset management is electronic article surveillance (EAS). For example, EAS tags are placed on electronic equipment, clothing, books, and many other consumer goods at retail outlets. After a customer purchases an item, the sales clerk deactivates the tag. If a person attempts to leave the shop, with unpurchased goods, readers at the doors detect the activated tag and trigger an alarm.

3.3.1.2 Tracking

Tracking applications are used to identify the location of an item, or more accurately, the location of the last reader that detected the presence of the tag associated with the item. Tracking systems require **more than one reader**, as well as a network, so that a central system can aggregate and correlate information received from each of the readers.

3.3.1.3 Authenticity verification

In authenticity verification applications, the tag provides evidence of the source of a tagged item. When readers subsequently query the tag, they can determine if it originated from a proper source. For authenticity verification systems to provide appropriate levels of assurance, they typically need to incorporate cryptography. *Digital signatures* based on cryptography are commonly used to authenticate a product. Moreover, they have the property of non-repudiation, which means the signatory cannot later deny creating the signature. Authenticity verification applications can use digital signatures to establish evidence of authenticity and enable later verification.

3.3.1.4 *Access control*

Access control systems use RFID to automatically check if an individual is authorized to physically access a facility (for example, a gated campus or a specific building), or logically access an information technology system.

There are two general types of access control systems: online and offline. Online systems have readers that are networked to a central computer. Since this system is networked, the central computer can provide updated access lists to the readers. In contrast, offline systems are not networked. In offline systems, the card lists the rooms that the holder can access, perhaps also listing an expiration date.

3.3.1.5 *Supply chain*

Supply chain systems can record information about products at every stage in the supply chain. Ideally, tags are affixed to products during the manufacturing process or soon afterward. As a product moves through the supply chain to the end customer, and later to post-sale service, the tag's identifier can be used by all supply chain participants to refer to a specific item. The information collected by a supply chain RFID system offers many benefits by more accurately tracking products *throughout their life cycle*. Such systems also generate an electronic pedigree for each item.

3.3.2 Application requirements

For any type of application, organizations should characterize the information to be processed by the system and determine the appropriate NFC / RFID devices and associated security controls. For this, they should consider:

- which data is considered sensitive or confidential
- whether data elements may be easily correlated or combined with other data to allow sensitive information to be inferred through indirect means
- how frequently this information is liable to change.

Data change over time is another important characteristic. In general, tag identifiers never change, but the data associated with the identifier can change. For example, in asset management, item information is typically written once and then does not change while the item remains in the system. However, in some cases, data changes frequently and is reused. When data elements change, the supporting technology must support write transactions and must have an access control mechanism to protect the integrity of the data (see Section 3.3.1.4: Access control). When an element does not change, it does not require this support.

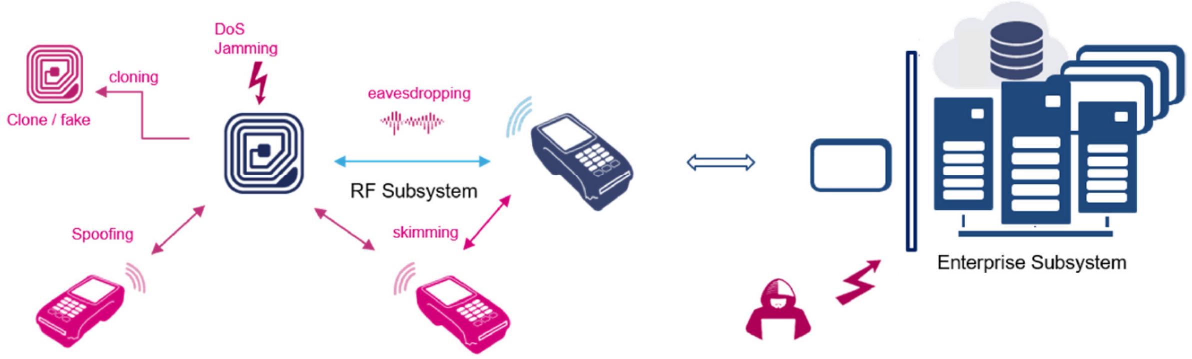
Organizations should therefore analyse which data is required to support the business process, and which elements must be modifiable. One important factor is whether tags and their identifiers are to be used once and discarded or reused.

The conditions under which readers query tags, such as the transaction speed, are a significant determinant of an RFID system's requirements. In some inventory applications, each transaction must be completed within a small fraction of a second or the process may take too long to finish. Many security mechanisms introduce latency into RFID transactions. Additional steps are needed to perform authentication, cover-coding, and other security-related procedures. Each additional step takes time. When considering security controls, organizations need to balance the business impact of each security control's effect on transaction speed with the protection it provides.

4 NFC/RFID risks

Selecting an ST25 tag and the security controls depends on the level of the threat in the environments in which the tags are expected to operate. Threats may be human or environmental.

Figure 3. Threats and risks



Human threats (intentional or unintentional) to tags include the ability to:

- damage or destroy a tag
- remove the tag from the item to which it is attached
- replace a tag with another
- clone a tag and use the clone for unintended purposes.

Environmental threats to tags include:

- extreme heat or cold applied to the tags
- moisture
- mechanical pressure, shock, and vibration
- radiation.

As with other technologies, organizations should assess risks, defined as the likelihood of a threat exploiting a vulnerability to cause an impact on the system.

Any risk assessment of environmental threats should also consider the impact of these conditions on the material to which the tag is attached and the glue or other mechanism that attaches the tag to the item. Impacts of harsh environmental conditions include: tag performance degradation, tag destruction, and separation of the tag from its associated item.

Organizations need to assess the likelihood of these threats in their environment, and set their RFID technology requirements accordingly. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users. In other IT systems, it is often easier to identify the occurrence of unauthorized behaviour, whereas with NFC/RFID systems a risk situation can occur even when processes are apparently functioning as intended.

Potential problems are not just limited to the RF subsystem. If the network supporting the RFID system is down, it is likely that the RFID system is also down.

NFC/RFID technology also raises important privacy concerns:

- Organizations might collect personal information for a particular purpose, and then later use that information for another purpose that is undesirable to the individual.
- Organizations implementing RFID systems to serve a particular business process might be unaware of how the RFID information might be used for unintended purposes.

In Europe, the GDPR regulation, scheduled to begin in May 2018, is intended to provide citizens of the European Union with greater control over their personal data, and assurances that their information is being securely protected by harmonizing data privacy laws across Europe.

It formalizes a series of new measures that apply to personal data including:

- breach notification
- the right to be forgotten
- right to access
- data portability
- privacy by design
- expanded definition of credentials.

Organization objectives often conflict with European privacy objectives. Organizations can benefit from the analysis and sharing of personal information obtained with RFID technology. At the same time, these activities may potentially violate the privacy rights or expectations of citizens and consumers. Similarly, methods to protect personal privacy may pose a business process risk.

Factors that impact the level of privacy risk include:

- Whether personal information is stored on tags
- Whether tagged items are considered personal, for example:
  - pharmaceuticals or devices that would reveal a medical condition, or a book that might reveal a political or religious affiliation
  - storage of credentials (personal information) or any assets that can be used, directly or indirectly, to identify the person, such as an RFID unique identifier.
- The likelihood of the tag being in the proximity of compatible readers
- The length of time records are retained in analytic or archival systems
- The effectiveness of RFID security controls, in particular:
  - the efficacy of tag memory access control and authentication mechanisms
  - the ability of tags to be disabled after their use in a business process has been completed
  - the ability of users to effectively shield tags to prevent unauthorized read transactions.

Organizations can rely on information published by an ST vendor through a European registration authority, to publish their privacy impact assessment process for NFC / RFID applications.

ST information, gathered in 'privacy capability statements', relates to the characteristics linked to the respect of private life proposed by the manufacturer. These can be 'standard' characteristics provided for by the various protocols (notably ISO) or proprietary characteristics.

5 Security controls

Organizations need to assess their risk exposure and choose an appropriate mix of controls for their environment, taking into account such factors as regulatory requirements, the magnitude of the threat, cost, and performance.

Two basic groups of RFID security-control risks are discussed:

- **Operational controls** involve the actions performed on a daily basis. RFID systems need operational controls that ensure the system physical security and their correct use.
- **Technical controls** use technology to monitor or restrict the actions that can be performed within the system. These include protecting data on tags, causing tags to self-destruct, and protecting wireless communications.

The information provided for each control includes:

- a description of the control and the control type
- tags where the control is supported and can be used
- benefits provided by the control
- limitations of the control and the residual risks.

This section does not cover security controls related to general IT systems, such as network infrastructure, databases, and web servers, which are discussed in the preceding sections.

5.1 Operational controls

5.1.1 IT securities at enterprise level

Control: IT securities in an enterprise subsystem describe the approach used in order to achieve high-level security objectives. This should cover each RFID subsystem, including network, database and application security in the enterprise. It should address:

- Access control to RFID information, especially records contained in RFID analytic system databases.
- Protection, including port and protocol restrictions for network traffic between the RF and enterprise subsystems.
- Password management, particularly with respect to the generation, distribution, and storage of tags' access, *lock*, and *kill* passwords.
- System security for readers and middleware, including the use and protection of SNMP.
- Management of associated cryptographic systems, including certification authorities and key management.

Type: Deterrence and preventive control.

Applicability: ST25Tx and ST25DV-xxx series

Benefits: IT securities govern the mitigation of human and environmental risks associated with the use of RFID technologies.

Limitations: IT securities need to be coupled with the implementation and enforcement of appropriate technical controls in order to be effective.

5.1.2 IT securities at RF level

Control: IT securities in the RF subsystem describe the approach used in order to achieve operational controls with RF components. This can include:

- Location of sensitive data. Instead of placing sensitive data on the tags, the data can be stored in a secure enterprise subsystem and retrieved using the tag's unique identifier.
- Physical access controls restrict access to authorized personnel where the RFID systems are deployed.
- Proper placement of RF equipment helps avoid interference and reduce hazards from electromagnetic radiation.
- Organizations can destroy tags after they are no longer useful, in order to prevent adversaries from gaining access to their data. This involves physically or electronically destroying tags, as opposed to just discarding them, when they are no longer needed to perform their intended function. Physical destruction may involve manual tearing or shredding using a paper shredder. Electronic destruction can be accomplished by using a tag Kill feature, or a strong electromagnetic field to render a tag's circuitry permanently inoperable.

Type: Preventive controls

Applicability: ST25Tx and ST25DV-xxx series

Benefits:

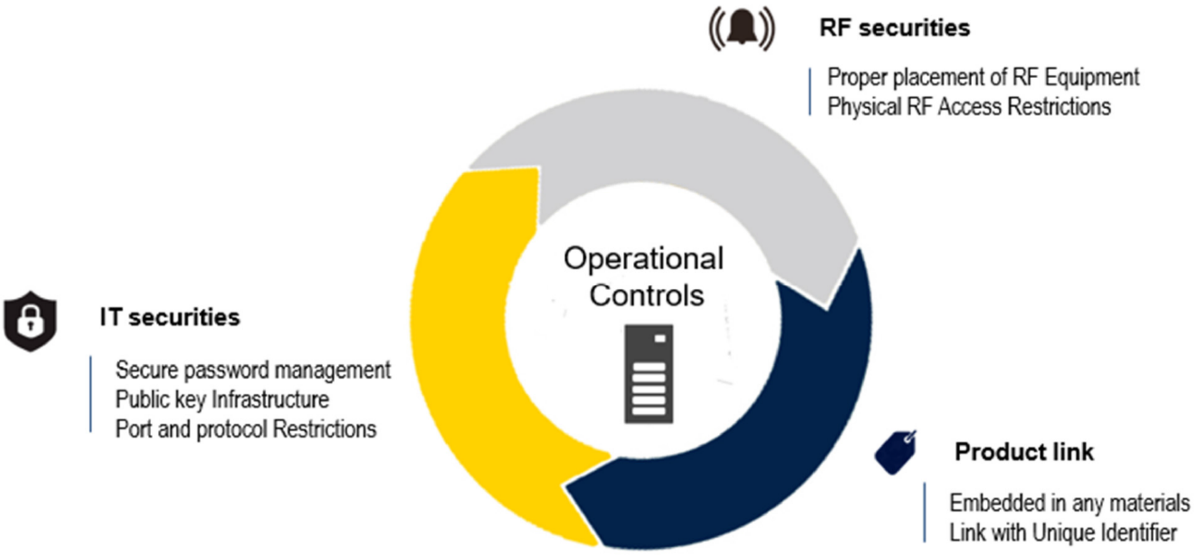
- Minimizing sensitive data on tags prevents that adversaries obtain information through rogue scanning or eavesdropping. Data encryption and their associated access control are often more cost effectively performed in the enterprise subsystem than in the RF subsystem.
- Physical access controls limit the ability of an adversary to get close enough to RFID system components to compromise RFID data security or to modify, damage, or steal RFID system components.
- Destroying or disabling tags eliminates the possibility that they could be used later for tracking or targeting and prevents access to sensitive data stored on the tags.

Limitations:

- Placing data in the enterprise subsystem makes the availability of the data conditional upon the network availability. Retrieving data over a network also introduces a small delay, which might be unacceptable for some applications.
- Physical access controls do not protect against attacks by insiders.
- Tag location cannot always be controlled, for instance when tags are used to track mobile items or items in transit. In some cases, this can be minimized with a metal foil or a sleeve that shields it from RF radiation when the tag/item is not used.
- Destruction of a tag prevents its use for future value-added applications such as post-sale product support, targeted recalls, or receipt-free returns.

Figure 4 provides the operational controls that ensure the physical security of the systems and their correct use.

Figure 4. **Operational control overview with ST25 NFC / RFID Tags**


RF securities
Proper placement of RF Equipment
Physical RF Access Restrictions
IT securities
Secure password management
Public key Infrastructure
Port and protocol Restrictions
Operational Controls
Product link
Embedded in any materials
Link with Unique Identifier

5.2 Technical controls

Several technical controls are currently available within the RF subsystems of ST NFC / RFID devices. Many of the technical controls listed are specified in standards, while others are available only in ST proprietary systems.

The RF subsystems generally include control types to:

- provide authentication and integrity services to RFID components and transactions
- protect RF communication between reader and tag
- protect the data stored on the tags.

5.2.1 Authentication and data integrity

The most common techniques for the RF subsystem of RFID systems are passwords, checksum or keyed-hash message authentication codes (HMAC), and digital signatures. In some cases, the primary objective of the authentication technology is to prevent unauthorized reading from or writing to tags. In other cases, the objective is to detect cloning of tags.

5.2.1.1 *Password authentication*

Control: ST25 NFC / RFID Tags do not permit *password-protected commands* to be executed unless they are accompanied by the correct password.

Protected commands may include those that support reading and writing of tag data, memory access control and the kill feature, or some other specific privacy-related features (that is, untraceable, silent and discreet features).

The secure password management system addresses all stages of the password, including generation, conveyance, and storage. The passwords are assigned to each tag in a physically secure environment to reduce the likelihood of eavesdropping, or the organization may use the *cover-coding mechanism* implemented in ST25 NFC / RFID Tags, for risk mitigation in insecure environments.

In the best cases, tags *should not share passwords*. In other words, organizations should not use a common password for multiple tags. This may not be administratively feasible in some environments, such as those in which the reader (offline framework) is not expected to have access to a networked database of tag passwords. In this condition, combining a UID and an administrator password may help. One administrator password is stored by the RF subsystem (reader side) and the reader encrypts and presents a combination UID/Master password to the tag (that is, diversification by UID). However, combining an administrator password with a *random value* is the best strategy to generate a specific password; effective password generation involves random selection of a password value.

Some ST25 NFC / RFID Tags can support several passwords for different purposes. For example, if separately accessible areas of memory use appropriately set commands for reading and writing to the tag. In the case where a tag has stored *several passwords* on the tag, access to a particular resource can be linked to a specific password. The reader needs to indicate which password needs to be used for authentication. Access to a resource on the tag is only granted when the reader has received the 'authenticated' state, through successful authentication with a specific password. To prevent any *DoS attack*, the *default value* of each password, delivered at the factory, should be changed by the organization, even if the password is not used by the application.

The protection level of the password feature can be improved by implementing a *security timeout*. An ST tag may introduce a time delay before it replies to the reader when the access attempt fails. ST25 NFC / RFID Tags offer this deterrence control, which can be combined with the detection of *anomalies in response time* to prevent spoofing attempts.

Type: Deterrence control

Applicability: ST25TA, ST25TV, ST25DV-PWM, and ST25DV-I2C series

Documentation: Table 10 references details of the use of password authentication in ST25 series devices.

Table 10. **Password authentication documentation**

Series	Part number	Reference
ST25TA	ST25TA02KB	**Datasheet** DS12365 [21] sections: • *Change reference data* • *Changing password*
ST25TV	ST25TV512 ST25TV02K	**Datasheet** DS12074 [19] - section: *Passwords and security sessions.*
	ST25TV512C ST25TV02KC	**Datasheet** DS13304 [22], section: *Passwords and security sessions.*
ST25DV-PWM	ST25DV02K-W1 ST25DV02K-W2	**Datasheet** DS12114 [20] - section: *Passwords and security sessions.*
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	**Datasheet** DS10925 [14] - ST25DV04K, ST25DV16K, ST25DV64K section: *Passwords and security sessions.*
	ST25DV04KC ST25DV16KC ST25DV64KC	**Datasheet** DS13519 [24] - ST25DV04KC, ST25DV16KC, ST25DV64KC section: *Passwords and security sessions.*

Benefits: The likelihood of tags being used for unauthorized purposes is greatly reduced.

Limitations:

- Passwords can be obtained through brute-force methods when the tag is limited to short passwords; long-range ST25 NFC / RFID Tags offer the possibility of using up to 64-bit passwords in some conditions, while short-range ST25 NFC / RFID Tags offer the possibility of using up to 128-bit passwords.
- Passwords can also be revealed through power-analysis attacks.
- In traditional IT systems, passwords are often changed on a periodic basis (for example every 90 days). In RFID systems, such changes may not be feasible, especially if the tags are not always accessible to the organization assigning the passwords.

5.2.1.2 *Digital signature*

Control: Digital signatures are based on asymmetric cryptography, also commonly referred to as public key cryptography.

ST25 NFC / RFID Tags have a permanent unique identifier than cannot be modified after manufacture. STMicroelectronics generates a public/private key pair, and obtains a corresponding public key certificate. A specified hash algorithm is used to compute a message digest of the tag's identifier, the message digest is encrypted with its private key to create a digital signature, and the resulting signature is stored on the tag. This digital signature, permanently locked into the device by STMicroelectronics, provides for non-repudiation of the tag chip. This embedded signature thereby proves that STMicroelectronics is the manufacturer of the tag.

The organization reads the signature by issuing a proprietary command, decrypts it with the ST public key, and computes the identical message digest to determine if a match exists. If the message digests match, the verification procedure provides assurance of the authenticity of ST25 NFC / RFID Tags.

Type: Detection control

Applicability: ST25TA, ST25TN, ST25TV, and ST25DV-PWM series

Documentation: See Table 11.

Table 11. **Digital signature documentation**

Series	Part numbers	Reference
ST25TA	ST25TA02KB	AN5101 [1] *TruST25™ digital signature for ST25TA512B, ST25TA02KB, ST25TA02KB-D and ST25TA02KB-P devices* (ST Restricted document)
ST25TN	ST25TN512 ST25TN01K	AN5660 [12] *TruST25 digital signature for ST25TN512 and ST25TN01K devices* (ST Restricted document)
ST25TV	ST25TV512 ST25TV02K	AN5104 [3] *TruST25™ digital signature for ST25TV512 and ST25TV02K devices* (ST Restricted document)
	ST25TV512C ST25TV02KC	AN5580 [9] *TruST25 digital signature for ST25TV512C and ST25TV02KC devices* (ST Restricted document)
ST25DV-PWM	ST25DV02K-W1 ST25DV02K-W2	AN5149 [7] *TruST25™ digital signature for ST25DV02K-W1 and ST25DV02K-W2 devices* (ST Restricted document)

Benefits: Digital signatures offer several advantages:

- Digital signature systems *do not require tags to store cryptographic secrets*. Tags are typically much more vulnerable to compromise than readers, so eliminating the need to store secrets on tags enhances overall system security. Each identifier is unique and so the digital signature is also unique. This ST digital signature is persistent, read-only, and is embedded with information during the manufacturing process.
- In many cases, digital signatures *do not require network connectivity* to successfully perform the authentication function. A reader may only need to store the public key certificate and the ST public key.

Limitations:

- A system of digital signatures requires a public key infrastructure (PKI), including registration and certification authorities, revocation functions, and associated policies and practice statements.
- Readers or middleware need to support digital signature verification algorithms, based on elliptic curves, such as 'secp128r1' that is commonly used by the TruST25 digital signature feature.
- ST digital signatures that are not dynamically generated by the tag are subject to replay attacks. An adversary could query a tag to obtain its evidence of authenticity (its digital signature), and then replicate that data on a cloned tag. Therefore, the digital signature usage should be coupled with operational controls (see Section 5.1.1: IT securities at enterprise level), when possible, to detect if several tags with the same UID are used in the system.
- No rewriting of a digital signature with an organization's public key can be done on ST25 NFC / RFID Tags. The ST digital signature is permanent and cannot be unlocked. However, an organization can generate its own digital signature after any operation and store its result in user memory or extra memory (depending on the ST25 NFC / RFID Tag product).

5.2.1.3 *Software-based authentication*

Control: Authentication can be performed by the analytic systems that are composed of databases, data processing applications, and web servers, and are based on smart risk analysis. Information such as time-stamp, geolocation, tag-related information (UID, counter tamper detect, digital signature) needed by the smart analysis may be retrieved from ST25 NFC / RFID Tags or NFC-enabled smartphones by means of downloaded applications, or simply by tapping the tag to interact.

Applications that require ‘proof of presence’, ‘time-and-attendance’, brand protection and other IoT applications using NFC-enabled smartphones may use this cloud-based scheme without the requirement of an external application.

The content of NDEF messages, such as URL, stored in an NFC Forum tag is usually static and can be read by an NFC-enabled smartphone without downloading an application. Augmenting NDEF messages with dynamic content that is modified by the tag provides additional information that is useful for the software-based authentication.

Type: Detection control

Applicability: ST25TN, ST25TVKC, and ST25DV-I2C series

Documentation: Table 12 references how the Augmented NDEF feature natively implemented in ST25TN and ST25TV02KC series tags can be used and how a microcontroller can enhance ST25DV-I2C series tags to provide an Augmented NDEF experience to end-users

Table 12. **Software-based authentication documentation**

Series	Part number	Reference
ST25TN	ST25TN512 ST25TN01K	**Application note** AN5680 [13] - Augmented NDEF messages with ST25TN512 and ST25TN01K devices,
ST25TV	ST25TV512C ST25TV02KC	**Application note** AN5658 [11] - Augmented NDEF messages with ST25TV512C and ST25TV02KC devices,
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	**Application note** AN5439 [8] - Augmented NDEF with ST25DV-I2C series Dynamic NFC Tags.
	ST25DV04KC ST25DV16KC ST25DV64KC	

Benefits: This control prevents any adversary from replacing a legitimate device with a fake device with an identifier unknown to the enterprise subsystem and allows any device that responds with inconsistent information, compared to the information already retrieved by the analytic system, to be inserted in the blocklist.

Limitations: Software-based authentication needs to be coupled with the implementation and enforcement of appropriate RF interface protection and data memory protection to be effective.

5.2.1.4 *Data integrity at rest*

Control: In several applications, the implementation of a data integrity strategy is mandatory.

Several strategies are possible, but whatever the solution used, extra memory density is required to hold the extra data:

- The *checksum* is perhaps the most commonly used method to prevent data loss, data corruption, and poor communication. It consists in computing a checksum of the data to write and in storing it into the user memory as an additional data byte. This can be computed for the whole user memory and for each specific memory area in user memory or for each sensitive asset stored in user memory, or internal tag-related assets (such as UID, counters, password, or lock bits or OTP bits after each expected and valid update). Checksums are particularly suitable for the secure communication of assets that are often read and updated.
- To give applications more robust, more elaborated checksum routines like *Keyed-Hash Message Authentication Code, HMAC* or ECDSA signature, can also be used to ensure the integrity of data stored in user memory or internal tag-related assets and evidence of the data ‘s authenticity.

- Data redundancy is also a good way of preventing data loss and data corruption into the tag memory or internal tag-related assets, more particularly adapted to the read-only data stored in the EEPROM. This on-board countermeasure is present in the nonvolatile EEPROM macrocell, implemented in ST25 NFC / RFID Tags. As the read-only data is never refreshed, there is a higher probability of facing a retention loss. With redundancy, there is a backup on each read-only byte.

Type: Preventive control

Applicability: ST25Tx and ST25DV-xxx series

Benefits: Applying the redundancy and the checksum strategy to write-once data improves the EEPROM robustness and, with it, data integrity.

Limitations: The management of HMAC keys provides similar challenges to those of password management and may not be practical if mobile readers do not have reliable access to an HMAC key management system. Additionally, to avoid replay attacks it is recommended to periodically update the symmetric or asymmetric keys.

5.2.1.5 *Seal integrity*

Control: ST25 NFC/RFID Tags series devices have a tamper-evident feature that helps prevent an adversary from altering the tags or removing them from the objects to which they are attached. This mechanism is simple and uses an *easily broken loop*. If the two TD pins are shorted with a wire, the loop is closed, and no tag tamper is detected. If the two pins are not shorted, the loop is open. The tamper state is automatically captured by the tag each time it is powered, and is available to readers on demand.

In the supply-chain application. this ensures that the tag has never been compromised or altered.

Note: With ST25 NFC/RFID Tags series devices, the tag is still operable even if the seal integrity is lost.

Type: Detection control

Applicability: ST25TV series

Documentation: Table 13 references details of seal integrity features in ST25TV series devices.

Table 13. **Seal integrity documentation**

Series	Part number	Reference
ST25TV	ST25TV512 ST25TV02K	**Datasheet** DS12074 [19] - ST25TV02K ST25TV512 section: *Tamper Detect*.
	ST25TV512C ST25TV02KC	**Datasheet** DS13304 [22] -ST25TV02KC ST25TV512C section: *Tamper Detect*.

Benefits: This control ensures that they have not been opened, manipulated, damaged, or subjected to extreme temperature, humidity, or shock.

Limitations:

- Sophisticated adversaries may be able to defeat the tamper resistance mechanisms. For example, a sophisticated adversary may be able to repair the loop during the RF power-off.
- Seal integrity needs to be coupled with the implementation and enforcement of appropriate physical or visual controls to be effective.

5.2.2 RF interface protection

Several types of technical control focus on the RF interface to tags, including:

- Error checking in air-interface can be monitored
- Cover-coding can be used to obscure the content of messages
- Data can be encrypted prior to its transmission
- The RF interface for tags can be temporarily shut off to prevent unauthorized access when the tag is not expected to be used for authorized purposes
- The RF interface may be turned off by default until a user takes action to activate it.

5.2.2.1 *Error checking in air-interface*

Control: An organization can set up error checking in the air-interface between the reader and the tag.

For example, readers can reject tag replies with anomalies in response times or signal power levels, which don't match the physical properties of the ST25 NFC / RFID Tag.

Or, more commonly, protection mechanisms against unintended failure, such as CRC, are included by RFID standards and allow detection of failures during RFID protocol communication for most sensitive tag operations, such as reading or writing data:

- Upon reception of a request from a reader, the ST25 NFC / RFID Tag verifies that the CRC value is valid. If it is invalid, the tag discards the frame and does not answer the reader.
- Upon reception of an answer from the ST25 NFC / RFID Tag, the reader should verify the validity of the CRC. In the case of an error, the readers can reject tag replies with CRC anomalies and some new actions are taken (a new query). Actions to be taken are the reader designer's responsibility.

Type: Detection control

Applicability: ST25Tx and ST25DV-xxx series

Benefits:

- If passive tags are used, the detection of response times can be a way to prevent spoofing attempts.
- The CRC is commonly used to detect failures during RFID-protocol communication, but can also be applied to internal memory structures to prevent the storing of faulty values. This control is discussed in Section 5.2.1.4: Data integrity at rest.

Limitations: Error checking may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.

5.2.2.2 *Cover coding*

Control: Cover-coding is a method for hiding information on the forward channel from eavesdroppers.

In ST25 NFC/RFID tags, cover-coding is used to obscure sensitive assets, such as passwords; the reader sends a query to the tag, the tag generates a random value and returns it to the reader. The reader produces the cipher text by applying an exclusive-or (XOR) operation of the password and the random value and sends the cipher text to the tag. The tag applies the XOR operation to recover the plain text or the password and check if it matches with the internal value.

Cover coding is an example of minimalist cryptography because it operates within the challenging power and memory constraints of passive tags. By itself, the XOR operation would be considered a trivial encryption algorithm in traditional cryptography, but it nonetheless mitigates risk to an acceptable level in many RFID environments, and against basic replay attacks.

Cover-coding is designed for RF subsystems in which the forward channel carries stronger signals than the back channel.

Type: Deterrence control

Applicability: ST25TV series

Documentation: Table 14 references details of how to calculate passwords to grant access rights to the user areas, modify the configuration of the device, or change the ST25TV512/02K feature modes.

Table 14. **Cover-coding documentation**

Series	Part number	Reference
ST25TV	ST25TV512 ST25TV02K	AN5103 [2] *Password encryption for ST25TV512 and ST25TV02K devices*
	ST25TV512C ST25TV02KC	DS13304 [22] ST25TV02KC and ST25TV512C datasheet, section *Password encryption*.

Benefits: Cover coding is useful when eavesdropping or basic replay attacks are a risk that requires mitigation, but adversaries are expected to be at a greater distance from the tags than readers.

Limitations: The effectiveness of cover-coding depends on the performance of the tag's random number generator.

5.2.2.3 *Encryption of data in transit*

Control: Data collected or processed are encrypted prior to over-the-air transmission. Applications that require an effective countermeasure to the threat of eavesdropping and for which cover coding offers inadequate protection may use the encryption-in-transit mechanism.

Type: Deterrence control

Applicability: ST25DV-I2C series

Documentation: Table 15 references details of how to develop an encrypted communication over NFC between a microcontroller and a smartphone using ST25DVxx-I2C series devices.

Table 15. **Data encryption in-transit documentation**

Series	Part number	Reference
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	AN5323 [5] *ST25DV-I2C crypto demonstration*
	ST25DV04KC ST25DV16KC ST25DV64KC	

Benefits: Encryption of data in transit prevents successful eavesdropping of over-the-air RFID transactions.

Limitations:

- Data encryption requires a key management system, which can be complex to manage and operate. Moreover, it is recommended to periodically update used cryptographic keys to avoid attacks.
- Cryptographic functions may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.

5.2.2.4 *Temporary deactivation of tags*

Control: The RF interface on some ST25 NFC/RFID tags can be turned-off temporarily. The method is different between simple and dynamic devices.

This control is most useful when communication between readers and a tag is infrequent and predictable. In a supply chain application, tags may be turned off to prevent unauthorized transactions during shipment. When the tags arrive at their destination, they are powered on again and managed. Conversely, tags used for in-transit visibility may be turned on for their trip. and turned off when they reach their destination.

- For ST25Tx series devices, access to the temporary deactivation feature is only granted when the reader has received the authenticated state, through a successful authentication with a specific password. The tag is unresponsive until it gets authenticated by a reader. RF commands are interpreted, but not executed in this mode. This is known as untraceable, discreet or silent mode.
- For ST25DV-xxx series devices, access to the temporary deactivation feature is controlled by the RF management feature, which can temporarily modify the behavior of the tags with the RF Sleep mode or the RF disable mode.

When RF Sleep mode is activated, all RF communications are disabled, the RF interface does not interpret commands, and minimizes the power consumption of the RF interface.

When RF disable mode is activated, RF commands are interpreted but not executed, and the tag responds with the error code 0x0F.

Type: Preventive control

Applicability: ST25TV and ST25DV-I2C series

Documentation: Table 16 references details of the ST25TV series temporary deactivation feature.

Table 16. **Temporary deactivation feature documentation**

Series	Part number	Reference
ST25TV	ST25TV512 ST25TV02K	DS12074 [19] ST25TV02K ST25TV512 datasheet, section: *Untraceable mode*

Series	Part number	Reference
ST25TV	ST25TV512C ST25TV02KC	DS13304 [22] ST25TV02KC ST25TV512C datasheet, section: *Discreet mode description* and section: *Silent mode description*.

The reference in Table 17 details how to manage simultaneous I²C and RF data transfer with an ST25DV-I2C series device.

Table 17. **Simultaneous I²C and RF data transfer documentation**

Series	Part number	Reference
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	AN5262 [4] *How to manage simultaneous I²C and RF data transfer with an ST25DVxxK device*
	ST25DV04KC ST25DV16KC ST25DV64KC	AN5624 [10] *How to manage simultaneous I²C and RF data transfer with an ST25DVxxKC device*

Benefits:

- Deactivating tags temporarily prevents unauthorized tag transactions during periods of inactivity
- This feature is also used to tackle privacy-related attacks for RF passive tags since UID or any assets that can be used, directly or indirectly, to identify the person, are not transmitted by the device.

Limitations:

- Even if the activation and deactivation process is automated, it introduces a delay that might not be acceptable for many time-sensitive applications.
- With passive tags, such as ST25TV series devices, the temporary tag deactivation can be turned off only by industrial readers, and never by a smartphone.

5.2.2.5 *Electromagnetic shielding*

Control: ST25 NFC / RFID Tags can be shielded with a container made of metal mesh or foil, known as a ‘Faraday cage’. Such containers prevent RF communication with ST25 NFC/ RFID Tags or block radio signals of certain frequencies to prevent RF communication with the tag, and thus protect tagged products from being detected or read by RFID readers.

This control is discussed in detail in Section 3.1.1: Main tag characteristics.

Type: Preventive control

Applicability: ST25Tx and ST25DV-xxx series

Benefits: Shielding limits the ability of eavesdroppers or unauthorized readers to collect data from an RFID system.

Limitations:

- Shielded containers require objects to be physically removed from the shielding material.
- Shielding might not work in some situations/applications. For example, it is difficult to wrap foil-lined containers around tags used in clothing for pets and people.
- Adversaries could use the Faraday cage principle to shield items from scanning by readers, to steal products without setting off security alarms (EAS alarms). Generally, adversaries might use a Faraday cage to render tags ineffective (DoS attack).

5.2.2.6 *RF energy adjustment*

Control: Organizations may adjust the level of transmitted RF energy from a reader. Additionally, the duty cycle of a reader can be controlled to prevent any risks of eavesdropping as discussed in Section 3.1.2: Main reader characteristics.

A protection may be added when using ST25 NFC / RFID Tags to prevent damage caused by wireless power chargers such as Qi or other inductive power transfer technologies, where the level of transmitted RF energy exceeds the limit value defined by the standard specifications.

This is an issue in applications where a system with NFC (for communication) is known to be placed within an inductive charger. An easy cost-effective solution is to add a series capacitance between the tag antenna and the tag IC.

Type: Preventive control

Applicability: ST25Tx and ST25DV-xxx series

Documentation: Table 18. RF energy adjustment documentation references details of how to protect certain ST25 NFC / RFID Tags from wireless power chargers.

Table 18. **RF energy adjustment documentation**

Series	Part number	Reference
ST25TA	ST25TA02KB	**Application note** AN5364 [6] - How to protect ST25 Tags from wireless power charging.
ST25TN	ST25TN512 ST25TN01K	
ST25TV	ST25TV512 ST25TV02K	
	ST25TV512C ST25TV02KC	
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	
	ST25DV04KC ST25DV16KC ST25DV64KC	

Benefits: Reducing the transmitted power can reduce the likelihood that an adversary can intercept communications.

Limitations: The drawback of reduced transmission power or duty cycle is performance degradation, especially with respect to back- channel communication from a passive tag. Also, changes in the physical environment can impact the power levels required for consistently successful transactions. Consequently, the benefits of power adjustments based on the survey site can be negated by changes to the environment.

This cost-effective solution is only applicable for Qi technology (frequency filtering out of 13.56 MHz), but not for WLC NFC Forum technology.

5.2.3 Tag data protection

Technical controls currently available for protecting tag data include:

- permanent tag memory access control, which can restrict use of tag commands and protect data stored in a tag's memory
- encrypting the data on tags
- the Kill feature, which can prevent subsequent unauthorized use of a tag
- tamper protection
- anti-tearing mechanism of some sensitive assets of a tag.

5.2.3.1 Tag-memory access control

Control: ST25 NFC/RFID tags support a password-protected lock feature that provides read and write protection to memory; the lock feature can be permanent or reversible.

ST25Tx series tags always have a permanent write lock feature that definitively changes the memory content to be only readable and makes it impossible to change the content after it has been written. Each memory block can be locked individually to prevent data to be modified. Leveraging this feature provides a very high level of protection since it is not reliant on a password and password management.

ST25Tx series tags may also contain an OTP area. This feature can be used to upgrade selected bits in an EEPROM block, only bits that are never updated in this block, are updated during a write command; other bits previously updated remain unchanged even if the write requests a change of these bits. Each memory bit can be locked *individually* to prevent data from being modified. This mechanism may be reversible with a specific reload mode. Leveraging this feature provides a very high level of protection since it is not reliant on a password and password management.

ST25Tx and ST25DV-xxx series tags also have reversible lock features. The memory is either read- and write-protected, or only write-protected, depending on the area configuration issued with a proprietary command. The memory may have several areas of user memory, each of which can be independently protected, and the area configuration can be locked if necessary. The effectiveness of tag memory access controls depends on proper management of passwords.

Section 5.2.1.1: Password authentication provides additional information on password authentication.

Type: Deterrence control

Applicability: ST25Tx and ST25DV-xxx series

Documentation: Table 19 references details of the permanent write-lock area.

Table 19. **Permanent write-lock area documentation**

Series	Part numbers	Reference
ST25TA	ST25TA02KB	DS12365 [21] ST25TA02KB datasheet, section: *Locking an NDEF file*
ST25TB	ST25TB512-AC	DS11495 [18] SR25TB512-AC datasheet, section: *OTP Lock Reg*
	ST25TB512-AT	DS11456 [16] SR25TB512-AT datasheet, section: *OTP Lock Reg*
	ST25TB02K	DS11469 [17] ST25TB02K, section: *OTP Lock Reg*
	ST25TB04K	DS11364 [15] ST25TB04K, section: *OTP Lock Reg*
ST25TN	ST25TN512 ST25TN01K	DS13433 [23] ST25TN512 and ST25TN01K datasheet, section: *Access restriction*
ST25TV	ST25TV512 ST25TV02K	DS12074 [19] ST25TV512 and ST25TV02K datasheet, section: *Lock Block*
	ST25TV512C ST25TV02KC	DS13304 [22] ST25TV512C and ST25TV02KC datasheet, section: *Lock Block*
ST25DV-PWM	ST25DV02K-W1 ST25DV02K-W2	DS12114 [20] ST25DV02K-W1 and ST25DV02K-W2 datasheet, section: *Lock Block*

The reference in Table 20 describes the resettable OTP area.

Table 20. **Resettable OTP area documentation**

Series	Part number	Reference
ST25TB	ST25TB512-AC	DS11495 [18] ST25TB512-AC datasheet, section: *Block 0 - 4: resettable OTP area*.

Table 21. **Reversible lock-area documentation**

Series	Part number	Reference
ST25TA	ST25TA02KB	DS12365 [21] ST25TA02KB datasheet, sections *Protecting an NDEF file* and *Protecting/Unprotecting an NDEF file*

Series	Part number	Reference
ST25TV	ST25TV512 ST25TV02K	DS12074 [19] ST25TV512 and ST25TV02K datasheet, section *Data protection*.
	ST25TV512C ST25TV02KC	DS13304 [22] ST25TV512C and ST25TV02KC datasheet, section *Data protection*.
ST25DV-PWM	ST25DV02K-W1 ST25DV02K-W2	DS12114 [20] ST25DV02K-W1 and ST25DV02K-W2 datasheet, section *Data protection*.
ST25DV-I2C	ST25DV04K ST25DV16K ST25DV64K	DS10925 [14] ST25DV04K, ST25DV16K datasheet, and ST25DV64K, section *Data protection*.
	ST25DV04KC ST25DV16KC ST25DV64KC	DS13519 [24] ST25DV04KC, ST25DV16KC, and ST25DV64KC datasheet, section *Data protection*.

Benefits:

- A write-protect *lock* command prevents the contents of a tag's memory from being altered
- A read-protect *lock* command prevents unauthorized users from reading or accessing the data on tags
- Leveraging the permanent lock feature provides a very high level of protection since it is not reliant on a password.

Limitations: Locking a tag's memory does not prevent data loss from electromagnetic interference or physical tag destruction. This control on sensitive asset such as OTP area or permanent write lock may be reinforced by additional controls, such as CRC, checksum, or even HMAC to detect any intended or unintended modification of lock bits (see Section 5.2.1.4).

5.2.3.2 *Encryption of data at rest*

Control: Data stored on a tag, in user memory, is encrypted before it is written to the tag. The control *does not require* that the tag encrypts or decrypts data. Instead, the encryption is performed by either the reader, middleware, or other enterprise subsystem components.

For example, the data can be encrypted with a *combination* of the UID and a secret key, before it is written on the tag. In this case, the tag's UID can be used to protect the data on the tag against interpreting and the secret key can be shared by all tags. Incorporating the UID also *prevents* cloning of a tag, for when the data of a tag is copied onto another tag, the data cannot be decrypted because the UID is different.

To enforce this protection, it is recommended to periodically update the encryption scheme (key or algorithm) to avoid replay attack or cloning.

Type: Deterrence control

Applicability: ST25Tx and ST25DV-xxx series

Benefits: Data encryption protects sensitive tag data from being read by individuals with unauthorized access to the tags.

Limitations:

- Data encryption requires a key management system. If the necessary key infrastructure is present in the enterprise subsystem, tag key management is quite easy to add. Otherwise, adding it is very complex.
- Sending tag data to network components for encryption or decryption is a source of network latency, which in conjunction with the time needed to complete cryptographic functions, may introduce an unacceptable delay in RFID systems.

5.2.3.3 *Kill feature*

Control: The kill feature is designed to protect consumer privacy by allowing tags to be disabled at the point of sale in retail environments. The kill feature allows a reader to render the tag unreadable, even though it remains attached to its associated item. The kill feature permanently disables a tag's functionality using a proprietary command. The kill command is protected using a 32-bit password different from the memory access password in the tag.

Section 5.2.1.1: Password authentication provides additional information on password authentication.

Type: Recovery control

Applicability: ST25TN and ST25TV series

Documentation: Table 22 references details of privacy-related control.

Table 22. **Privacy-related control documentation**

Series	Part numbers	Reference
ST25TN	ST25TN512 ST25TN02K	DS13443 [23] ST25TN512 and ST25TN02K datasheet, section *Privacy: kill feature*
ST25TV	ST25TV512 ST25TV02K	DS12074 [19] ST25TV512 and ST25TV02K datasheet, section *Kill feature description*
	ST25TV512C ST25TV02KC	DS13304 [22] ST25TV512C and ST25TV02KC datasheet, section: *Kill feature description*

Benefits:

- Using the kill feature prevents a tag from being reused improperly. For example, discarded tags that have not been disabled may be read by adversaries to gain access to data, such as which products an organization or individual is purchasing or using.
- This feature is also used to tackle the privacy-related attacks.

Limitations:

- If an adversary who learns the kill password, improperly disables tags that should remain in operation, the supported application no longer functions properly. This risk is particularly salient for organizations that assign the same password to multiple tags because doing so could enable an adversary to disable large numbers of tags with a single compromised password. So, the password diversification is highly recommended for this feature.
- Once killed, a tag cannot be used for any further application involving the asset (for example recalls, receipt-less product returns).
- Data stored on the tag is still present in the memory after it is killed (although it can no longer be accessed wirelessly), and therefore can be accessible to someone with physical access to the tag.

5.2.3.4 *Antitearing protection*

Control: The antitearing mechanism provides the verification of data integrity and data consistency when the tag is pulled out of the reader field or if the tag has not enough power to complete a write-alike operation. This includes data backup and shadow-memory techniques that allow the recovery of data when the tag is powered up the next time after the occurrence of an interruption.

ST25Tx series tags apply this protection to sensitive assets, such as counters. For example, the counters are mandatory for transportation applications, which require only the incrementing of the value of the counters, or the latest value to be kept, but the counter is never read with an undefined or unintended value.

Type: Recovery control

Applicability: ST25TA, ST25TB, ST25TN, and ST25TV series

This feature is always enabled when the counters are activated and does not require any user programming.

Benefits: This recovery protection is automatically enabled when the counters are activated.

This is not suitable for applications that require strict counting without loss of increment.

Limitations: this approach might not work in some situations/applications. This is not indeed suitable for applications that require strict counting without loss of increment. It may not be sufficient in the applications that are often faced daily human threats and risks such as fraud. Certain enhanced attacks to cause an impact on the security automatic mechanism and to exploit vulnerability may occur and need to be thwarted by combining technical controls since ST25 series are not considered as security certified products and may not resist to advanced attacks.

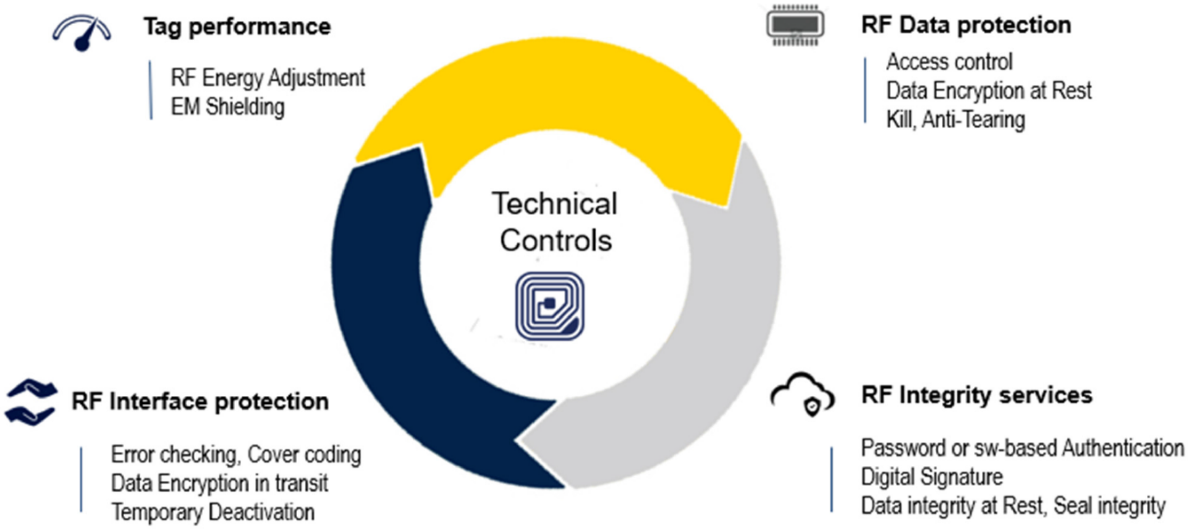
To reduce the chance of unintended manipulation or fraud, additional protections are recommended:

- The implementation of data integrity at rest (refer to Section 5.2.1.4) can be used to prevent data corruption after the last update of the internal asset.

- The addition of a diversification scheme by using the UID asset of the device: either in CRC, CMAC, HMAC computation or either in key diversification if cryptographic algorithms for integrity and authentication are used.
- The integrity digest code calculated outside the device should be stored in a reversible lock area in the user memory. If this reversible mechanism is not present in the device, data redundancy can also be used with the encryption and authentication scheme at rest.
- Additional operational control at system level/online should be implemented to detect any suspicious counter value and allow UID repudiation in this case.

Figure 5 shows all the technical controls offered by ST25 NFC / RFID Tags.

Figure 5. ST25 NFC / RFID Tag technical control overview



6 Conclusion

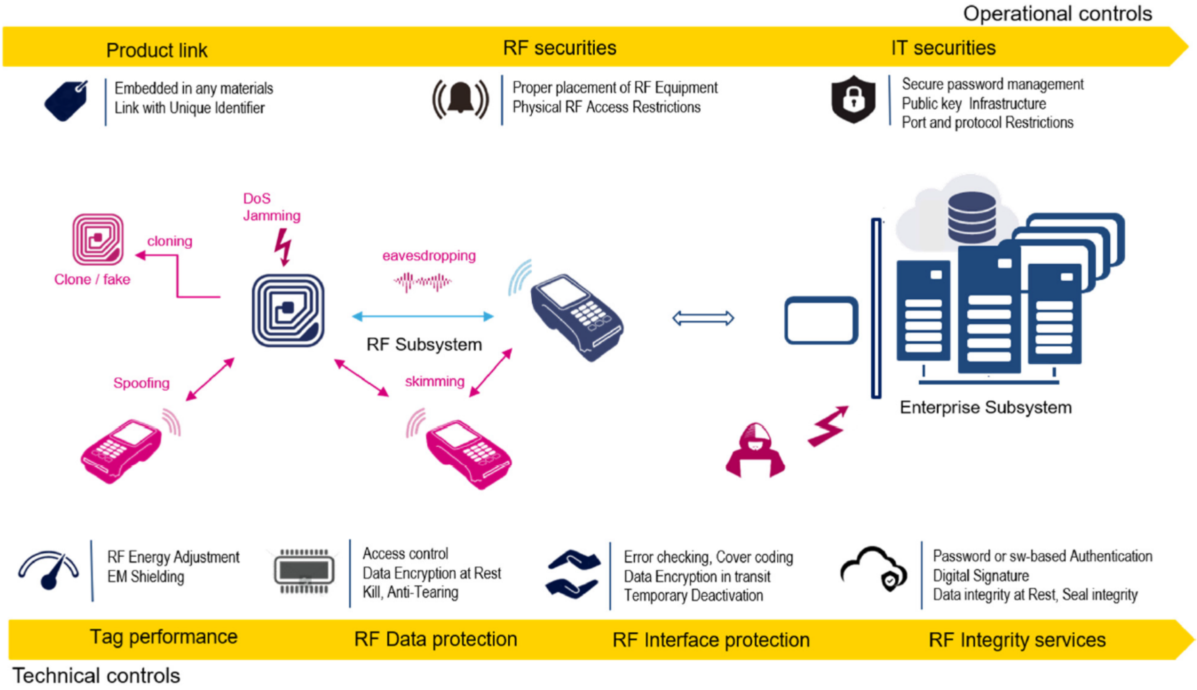
The RF and enterprise subsystems allow an RFID system to support the business of organizations. The components of these subsystems allow an RFID system to be tailored to the needs of a particular application.

Understanding the major component characteristics of the RF system can help organizations identify weaknesses or threats, and the appropriate controls required in their environments and applications. Failures in any component or subsystem of the RFID system can result in system-wide failure.

Organizations should use a combination of operational and technical controls to mitigate the risks of implementing RFID systems. Because each implementation is highly customized and requirements are different, the security controls mentioned in this document are not all applicable or effective for all RFID applications.

Privacy considerations are interrelated with security considerations. Organizations may require the implementation of privacy controls to comply with the laws and regulations.

Figure 6. **Overview of ST25 NFC/RFID tag security and privacy tag capabilities**



Thanks to its broad ST25 product portfolio, STMicroelectronics can help organizations choose an appropriate mix of controls for their applications and their environments, taking into account factors such as component characteristics, regulatory requirements, magnitude of the threat, cost, and performance.

Revision history

Table 23. **Document revision history**

Date	Version	Changes
19-Jun-2020	1	Initial release.
23-Jan-2024	2	Document updated with new product introduction.
15-Apr-2024	3	Updated: • Table 1. Applicable products • Table 10. Password authentication documentation • Table 11. Digital signature documentation • Table 18. RF energy adjustment documentation • Table 19. Permanent write-lock area documentation
09-Aug-2024	4	Updated Section 5.2.3.4: Antitearing protection. Minor text edits across the whole document.
13-May-2025	5	Updated: • Section 5.2.1.1: Password authentication • Section 5.2.2.4: Temporary deactivation of tags

Contents

List of tables

List of figures