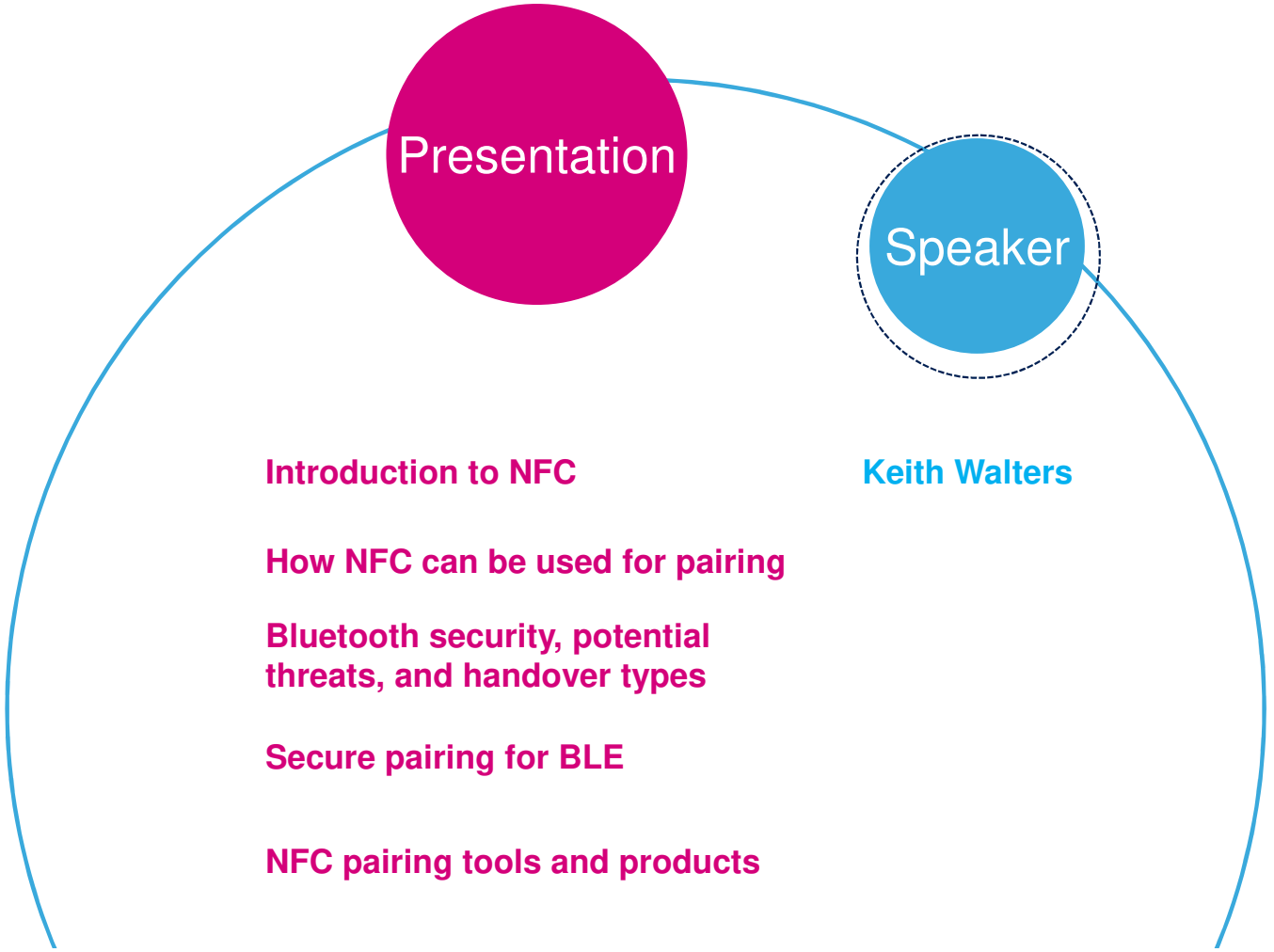
Secure Bluetooth Pairing Made Easy with NFC

Jim Barlow
RFID and Memory Division

life.augmented

Technology Tour 2019
Vancouver, BC | September 24

Agenda



life.augmented

NFC for Bluetooth Pairing

life.augmented

NFC Technology Overview

Bluetooth/WiFi pairing, access control, payments, ticketing…

- Near Field Communication, a short range Radio Frequency Identification (RFID) wireless technology
  - Operating at 13.56MHz High Frequency band
  - Based on the HF RFID standards ISO14443A/B, ISO15693, FELICA
- NFC operating modes
  - Read/Write (reader-to-passive tag/card)
  - **Card Emulation (e.g. Apple Pay, Android Pay, Samsung Pay, etc.)**
  - **Peer-to-Peer (i.e. reader-to-reader)**
- Maximum data transfer rate is 424 kbps (P2P)
  - Proprietary reader modes can go up to 6.8 Mbps
  - Tag data rates vary from 27kbps to 106kbps
- Defined Tag Types
  - Various combinations of features, storage and security
  - Types 1-5. ST offers Type 4 & 5 (the most popular)
- NFC is maintained by the NFC Forum
  - Ensures Interoperability between devices
  - Standardized use cases (web link, Bluetooth handover,…)

life.augmented

iOS13 NFC capabilities

- Provided support for **reading/writing** tags using native commands
  - NFC Type 5 - ISO15693 : Implemented **full set + extended** commands as defined in ISO15693-3 standard
    - Read/Write single/multiple blocks
    - Custom Commands : ST25 Password, TruST25 Digital Signature, Fast Transfer Mode, PWM settings, Tamper Detection…
  - NFC Type 4 – ISO14443A read/write commands
    - Ex : ST25TA TruST25 Digital Signature management
  - Smart Card read/write commands
  - FeliCa read/write commands
- Added support for **writing** NDEF messages across different tags from Type1 up to Type 5
- Ability to **permanently lock** an NFC tag that has been encoded with an NDEF message
- Additional enhancements to Apple Pay for NFC
  - iOS13 comes with new feature for processing Value Added Service (VAS) tags. This feature is still unclear at the moment. More details to come later…

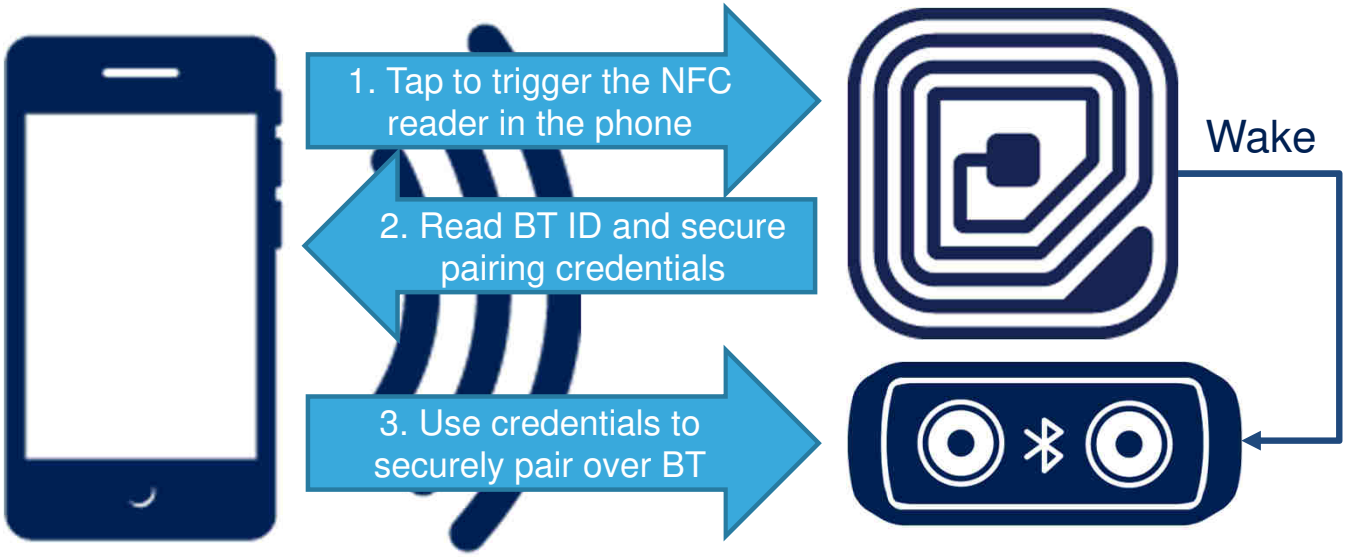
How does NFC help with Bluetooth pairing?

- There are a number of ways to pair two Bluetooth devices (e.g. PIN numbers, numerical comparison, etc.).
- One method is called Out Of Band (OOB) pairing. QR codes and NFC are two examples of OOB pairing mechanisms.
- With a simple tap, a smart phone can read the pairing information off of a NFC tag and use it to automatically pair with a BT device. No other input is needed!

life.augmented

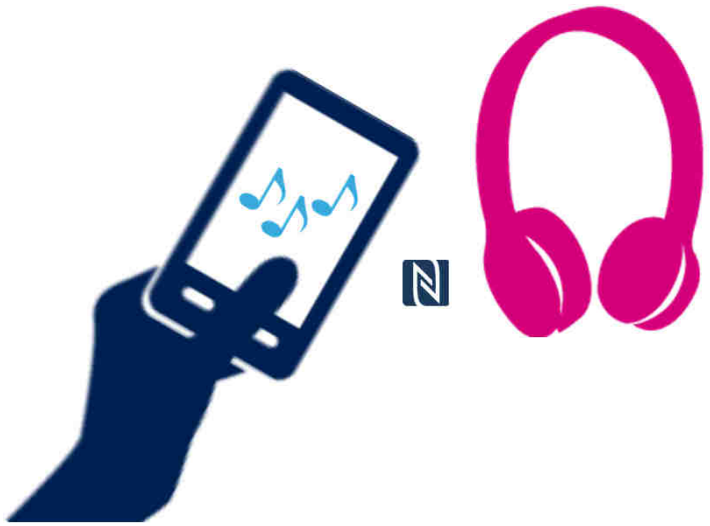
How does NFC pairing with BT work?

NFC simplifies the pairing process



Benefits to end-customer

- Faster and simpler – no need for BT/Wi-Fi sub-menus or searching through lists to find surrounding devices
- No conflicts – pair only the devices you intend to pair
- Secure communications – encrypt a BT link by exchanging credentials securely with just a tap
- Low cost - ideal for BT devices that are too small or cannot afford a user interface for PIN or password entry
- Ease of use - unlike QR codes, Line of Sight is not required with NFC
- Save power – use NFC to automatically turn on a battery-powered BT device and instantly pair



How is pairing information stored?

The NDEF Record Format

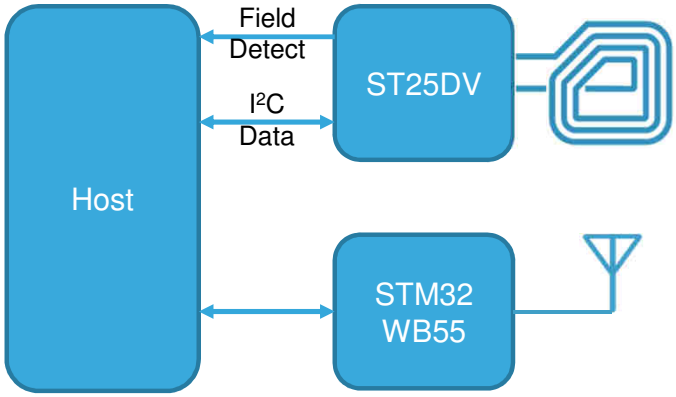
- NFC Data Exchange Format (NDEF) is a standard format defined by the NFC forum to store data on a NFC tag
- Different types of NDEF records :
  - SMS (Short Messaging Service)
  - URI (Universal Resource Identifier)
  - Text
  - Bluetooth Pairing (***handover***)
  - Smart poster….
- The type of NDEF record is defined by the Record Type Definition (RTD) field, located in the NDEF header. A Well Known Type (WKT) of NDEF record used for Bluetooth handover is a MIME (Multipurpose Internet Mail Extensions) type

→ for detailed Info for NDEF record structure, please refer to the Technical Specifications of the NFC Forum!

life.augmented

Tags for Bluetooth pairing

Dynamic I²C Tags



Flexible Solution

- Can implement dynamic MAC addressing
- Can identify current carrier power states
- Power up BLE when NFC field detected
- Can create new keys and randomizers after every pairing

ST Offerings

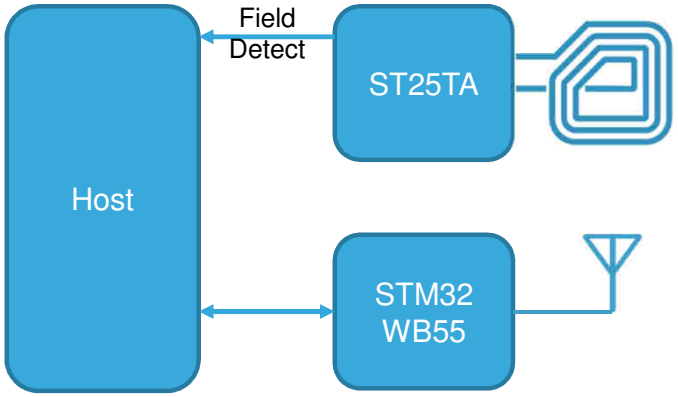
- ST25DV
- M24SR

Example application: Wearable Patient Monitor. A nurse can tap their tablet to the monitor to securely download a log of the last several hours of collected heat rate, blood pressure, etc. data. A while later, a doctor could do the same with a different set of security keys.

life.augmented

Tags for Bluetooth pairing

NFC Tags with Field Detect



Power Efficient

- Only power-up BLE when NFC field detected
- Cannot implement dynamic addressing
- Cannot update secure pairing information
- Must advertise all carriers (capabilities)

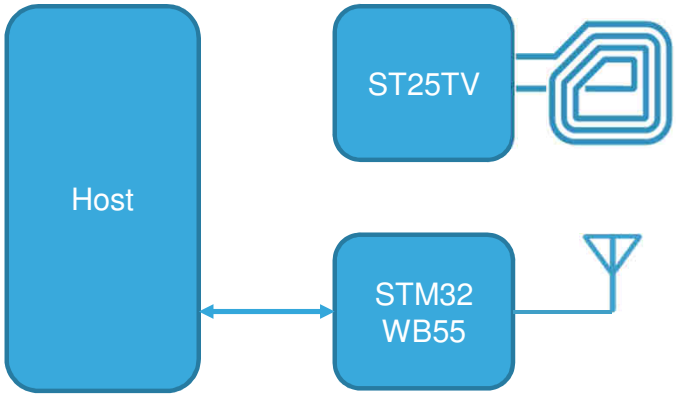
ST Offerings

- ST25TA02K-P

Example application: Low cost Bluetooth speaker for playing music. By tapping your phone to the speaker you can power the device on and starts the pairing process. This eliminates the need for a power button. Device authentication isn't as critical in this case.

Tags for Bluetooth pairing

Standalone NFC Tags



Low Cost

- Can only store basic pairing information, no authentication data for secure pairing
- Cannot wake the BLE radio on field detect
- Cannot implement dynamic MAC addressing
- Must advertise all carriers (capabilities) regardless of their current power state

ST Offerings

- ST25TA
- ST25TV

Example application: Low cost (always on) environmental monitor. The tag stores the Bluetooth address and device role making pairing easy. Also, the tag could be added “after-the-fact” with no wiring to the radio required

BR/EDR and LE Feature Comparison

Different versions of Bluetooth have different security methods

Characteristic	Bluetooth BR/EDR			Bluetooth Low Energy	
	Prior to 2.1	v2.1 to v4.0	v4.1 and beyond	v4.0 and v4.1	V4.2 and beyond
RF Channels	79 channels with 1MHz spacing			40 channels with 20MHz spacing	
Discovery Method	Inquirery/Paging			Advertising	
Max Piconet Slaves	7 active / 255 total			Unlimited	
Device Address Privacy	None			Private Addressing	
Max Data Rate	1 – 3 Mbps			1 Mbps (GSMK)	
Output Power/Range	100mw (20dBm) / 30M			10mW (10dBm) / 50M	
Security Version	BR/EDR Legacy	Secure Simple Pairing	BR/EDR Secure	LE Legacy	LE Secure
Pairing Method	SAFER+ (E21 & E22)	ECDH P-192 HMAC-SHA-256	ECDH P-256 HMAC-SHA-256	TK and STK with AES-128	ECDH P-256 HMAC-SHA-256
Device Authentication	SAFER+ (E1)	SAFER+ (E1)	HMAC-SHA-256	AES-CCM	AES-CCM
Encryption	SAFER+ (E0)	SAFER+ (E0)	AES-CCM	AES-CCM	AES-CCM

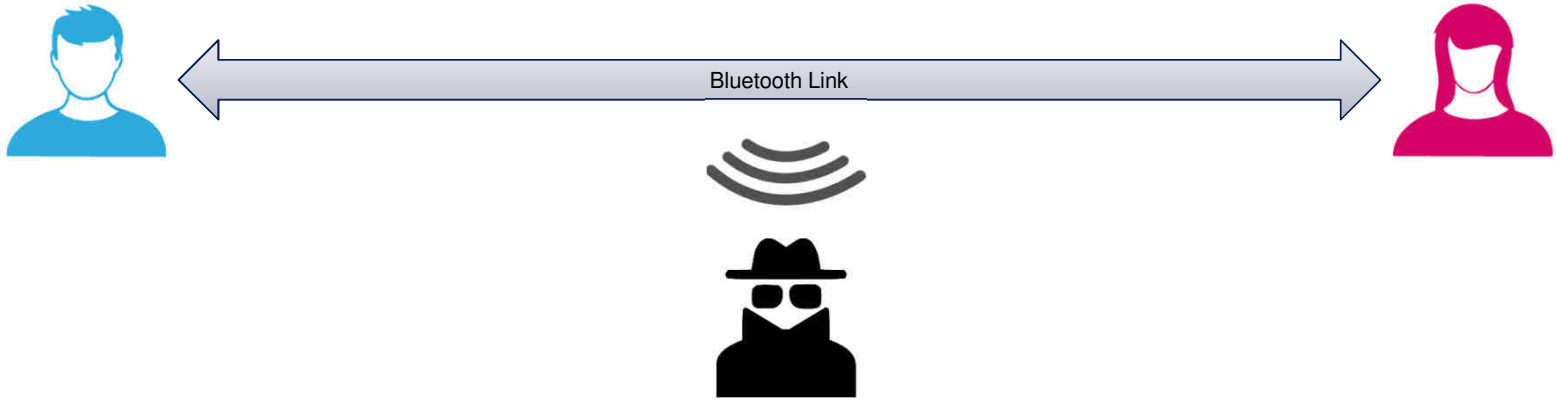
life.augmented

BR/EDR Secure and LE Secure together are known as Secure Connections

Bluetooth Security Threats

Passive Eavesdropping

Passive eavesdropping is where a third party listens in to the data being exchanged between two paired devices. NFC overcomes this by providing a larger encryption key (LE Legacy) and, with its inherently short range, NFC can be used to securely transfer credentials used for secure pairing.



life.augmented

Bluetooth Security Threats

Man In The Middle

MITM (i.e. active eavesdropping) is a process by which a third party impersonates the Initiator and Responder, in order to trick them into connecting to it. The BLE central and peripheral devices will connect to the malicious party which intercepts all data being sent between them. The malicious party can also insert false data or remove data before it reaches the recipient. NFC provides the highest level of resistance to MITM attacks due to its short communications range and 128-bit key size (LE Legacy).

BT pairing process – overview

Pairing is a three-phase process for establishing keys used for secure communications. The first two phases are always used and may be followed by a 3rd optional phase for transport specific key distribution

- **Phase 1 – Feature Discovery**: The two devices tell each other what their capabilities are by reading their Attribution Protocol (ATT) values. These determine which pairing method is used in phase 2, what the devices can do and what they expect.
- **Phase 2 – Key Agreement / Generation:** For Secure Connections pairing, both devices create a Diffie-Hellman Key and use it to derive a shared Long Term Key (LTK).
- **Phase 3 – Key Distribution:** The key from phase 2 is used to distribute any other keys needed for communication. Examples of other keys are the Connection Signature Resolving Key (CSRK) for data signing and the Identity Resolving Key (IRK) to decrypt the Random Private Resolvable address (used by iOS devices)

Bonding devices store encryption keys for later secure communication.

Bluetooth Pairing Methods and Mechanisms

The introduction of Secure Simple Pairing in BT v2.1 defined 4 types of pairing methods: Just Works, Passkey, Numeric Comparison and Out Of Band.

- Just Works: No key entered. Good for devices with no user input like sensors. No MITM protection.
- Passkey Entry: Six digit PIN code
- Numeric comparison (LE Secure): When both devices have a display. If the same number shows up on both displays, the user would confirm a match
- Out of band: Use of an alternative communications channel (NFC or QR code) to execute a handover by exchanging authentication data and Bluetooth MAC IDs

For LE Legacy Pairing (v4.0 and v4.1)

- No Numerical Comparison equivalent
- Just Works and Passkey Entry do not provide any passive eavesdropping protection. This is because Secure Simple Pairing uses Elliptic Curve Diffie-Hellman (public-private key pairs) and LE legacy pairing does not

NFC Handover Terms

Handover Requestor (Initiator)

NFC Forum device that initiates the handover operation. The requestor is also sometimes referred to the “master”

Handover Selector (Responder)

NFC Forum device or NFC Forum Tag that responds to the Handover Requestor. The selector is sometimes referred to as the “slave”

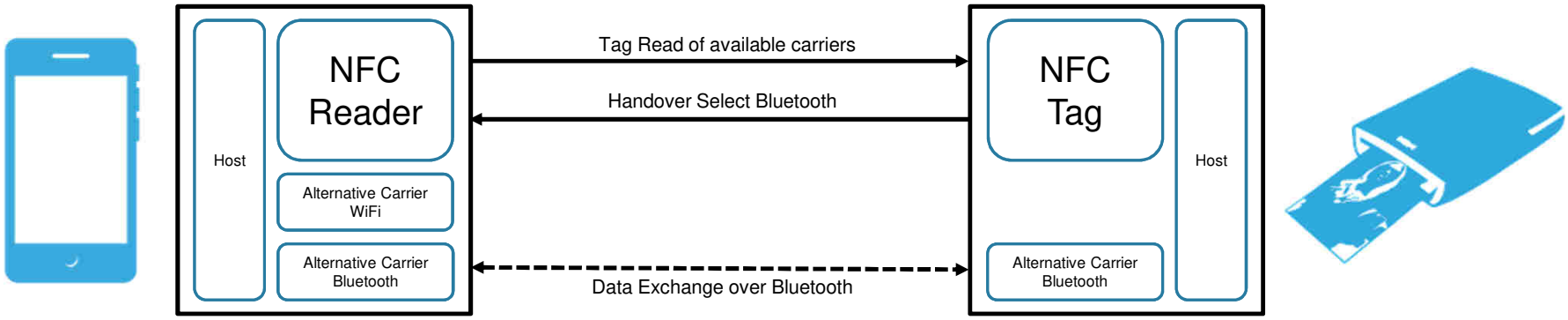
Handover Mediator

NFC Forum device that can facilitate connection between two other NFC enabled devices. An example would be a smart phone used to configure a wireless network.

NFC Handover Types

Static Handover

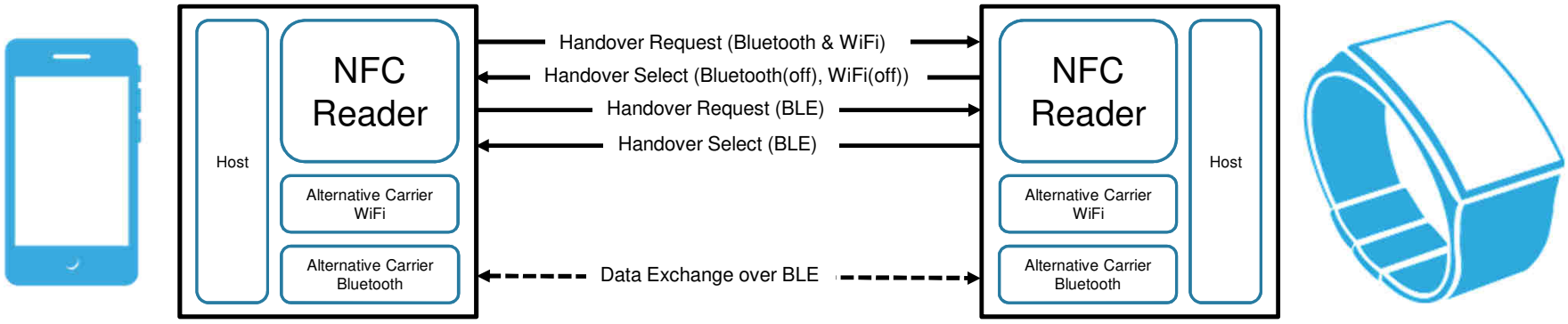
- Used in cases where the Handover Selector (responder) device is equipped with a NFC Forum Tag only. The initiator reads the MAC ID of the responder along with some descriptive info about the responder's role.
- Due to the static nature of data on a tag, a pre-stored Handover Select Message will have to indicate all available carriers since the tag is not capable of constructing a dynamic Handover Select Message.
- Simple Secure Pairing is NOT supported due to the static nature of the tag. Pairing key should be regenerated every time.



NFC Handover Types

Negotiated Handover

- Used in cases where the Handover Responder device is an active NFC Device (e.g. Reader or Dynamic Tag)
- The device can selectively advertise available carriers. In the example below the Selector is power constrained. The requestor asks for BLE and WiFi but the Selector only offers BLE in this case.
- Dynamic Handover can support optional secure pairing

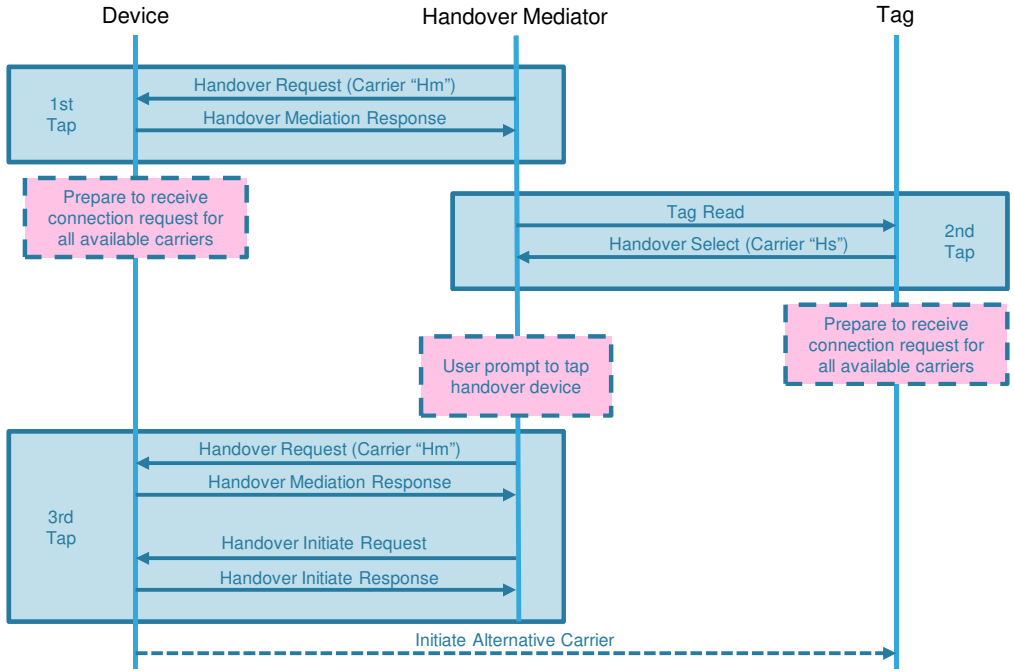


life.augmented

NFC Handover Types

Mediated Handover – Static Tag Example

- Exchange of NDEF messages between two NFC-enabled devices via a third NFC device (i.e. the Handover Mediator). The mediator serves to get both devices to agree on one or several alternative carriers (e.g. a cell phone used to commission a network of NFC-enabled wireless sensors)
- Can support optional secure pairing if both devices have active NFC transceivers, or one has a dynamic tag.



life.augmented

LE Secure Pairing

life.augmented

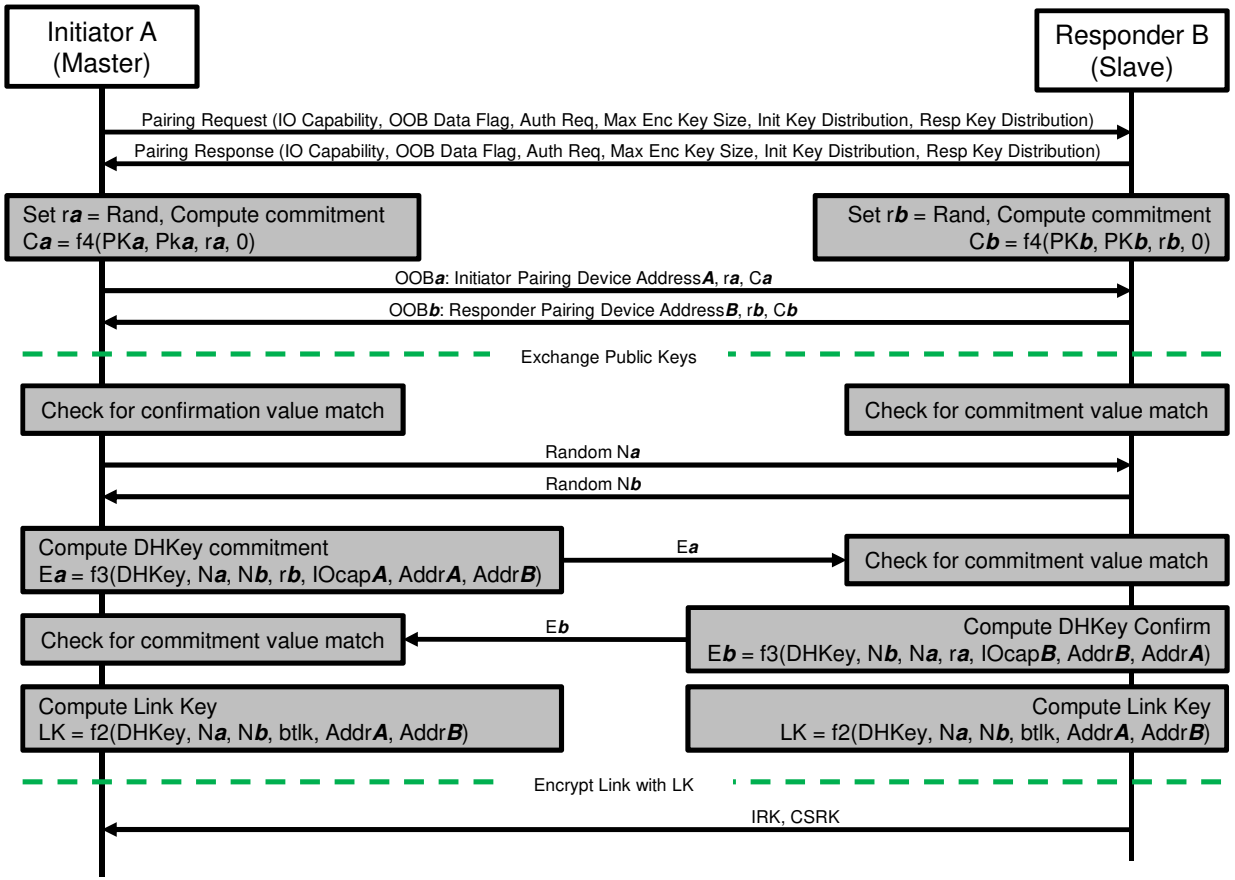
OOB LE Secure Pairing Process

Dynamic Handover

Phase 1: Pairing Feature Exchange

The devices identify which of the 4 methods of pairing are available, which also defines the Temporary Key (TK) used for authentication:

- Just Works
- Passkey
- Numerical Comparison
- Out of Band – This option is used if the OOB flag is set in both the Pairing Feature Request and Response



life.augmented

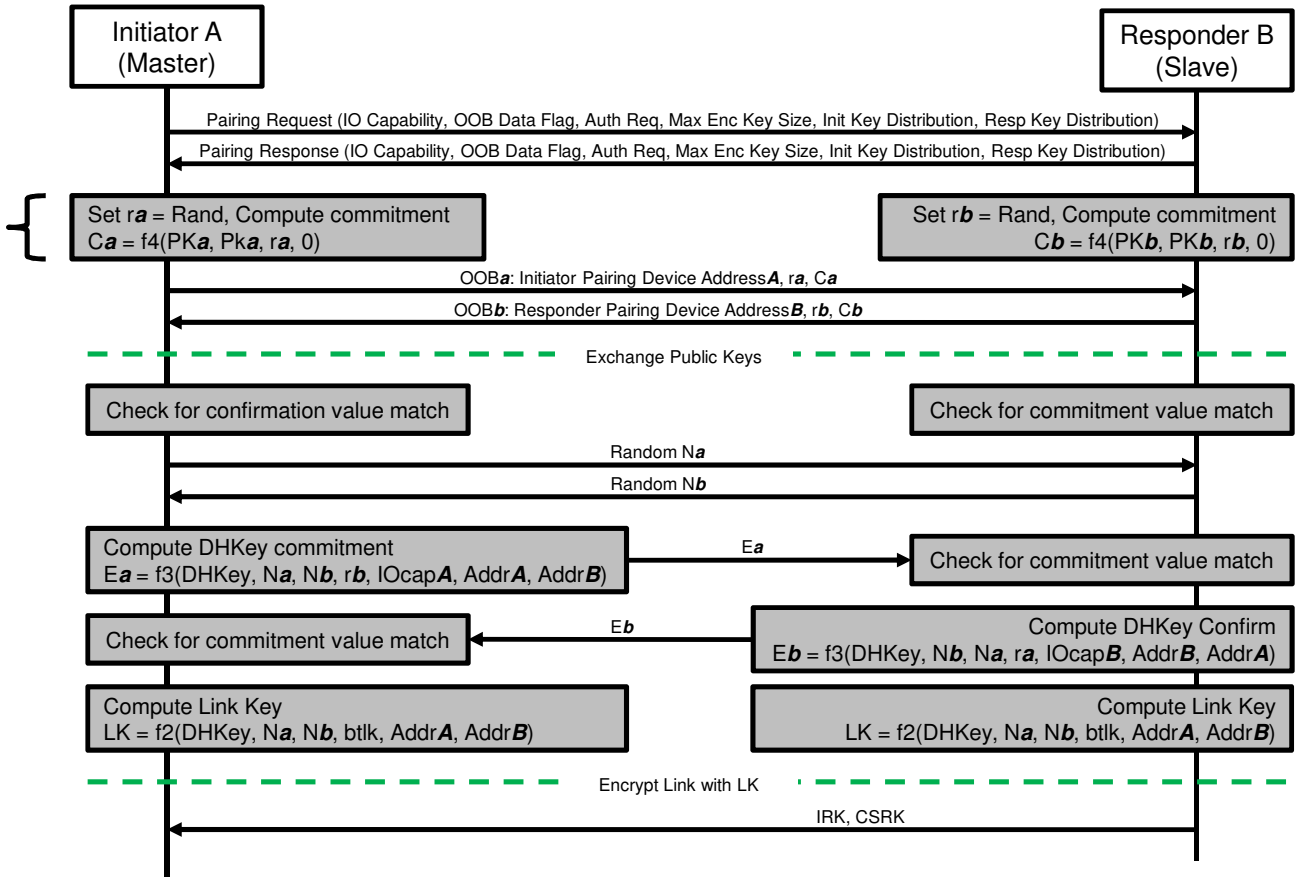
OOB LE Secure Pairing Process

Dynamic Handover

Phase 2: Key Agreement

Step 1: Both the master and slave generate “commitments” which is a Hash of a random number with the device’s public key.

A commitment scheme allows you to commit to a certain value without revealing it until a later date



life.augmented

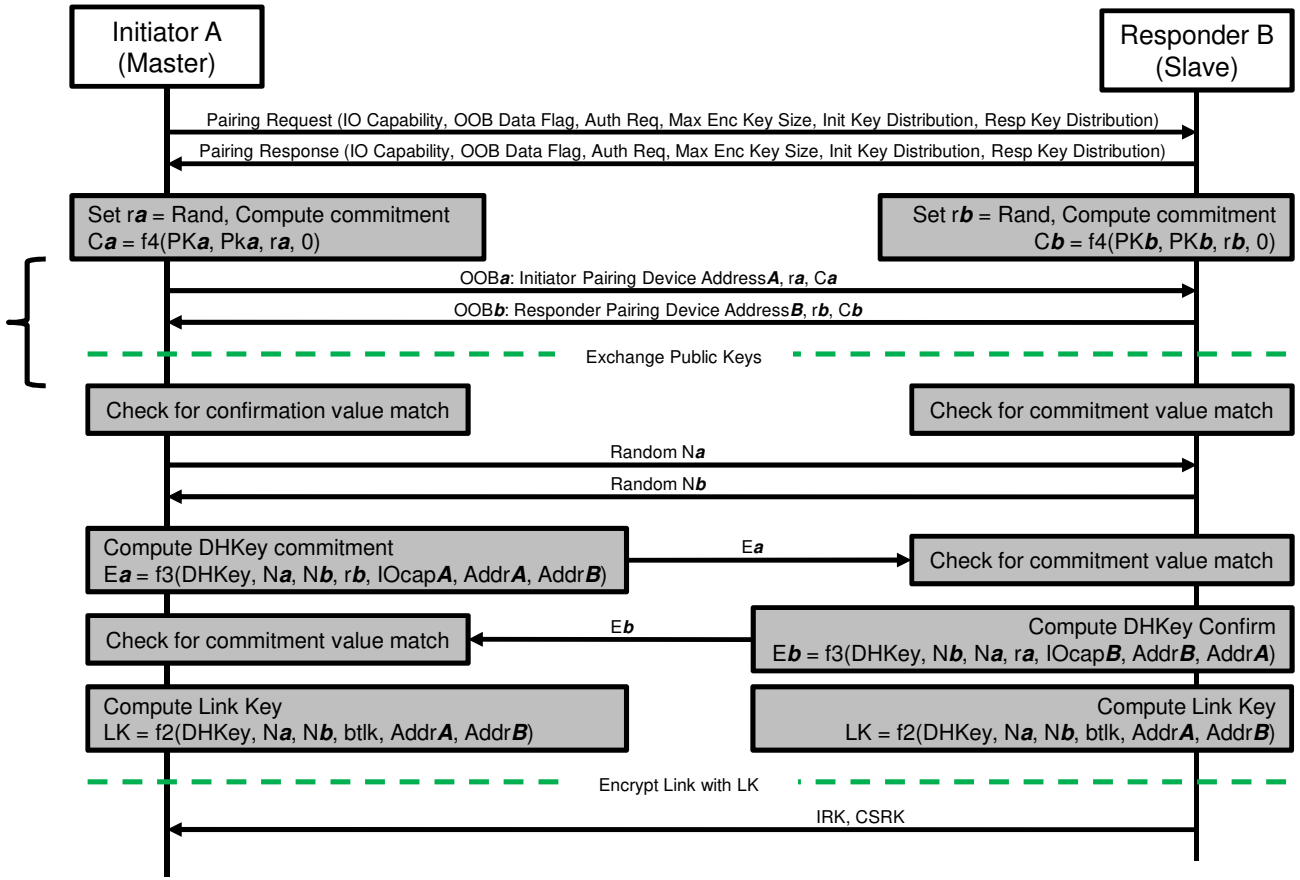
OOB LE Secure Pairing Process

Dynamic Handover

Phase 2: Key Agreement

Step 2: Using NFC, the master and slave exchange their “commitments” as well as the random number used to generate the commitment and their MAC Address.

This is also the point where the master and slave would exchange their public keys over Bluetooth if the pairing was NFC triggered



life.augmented

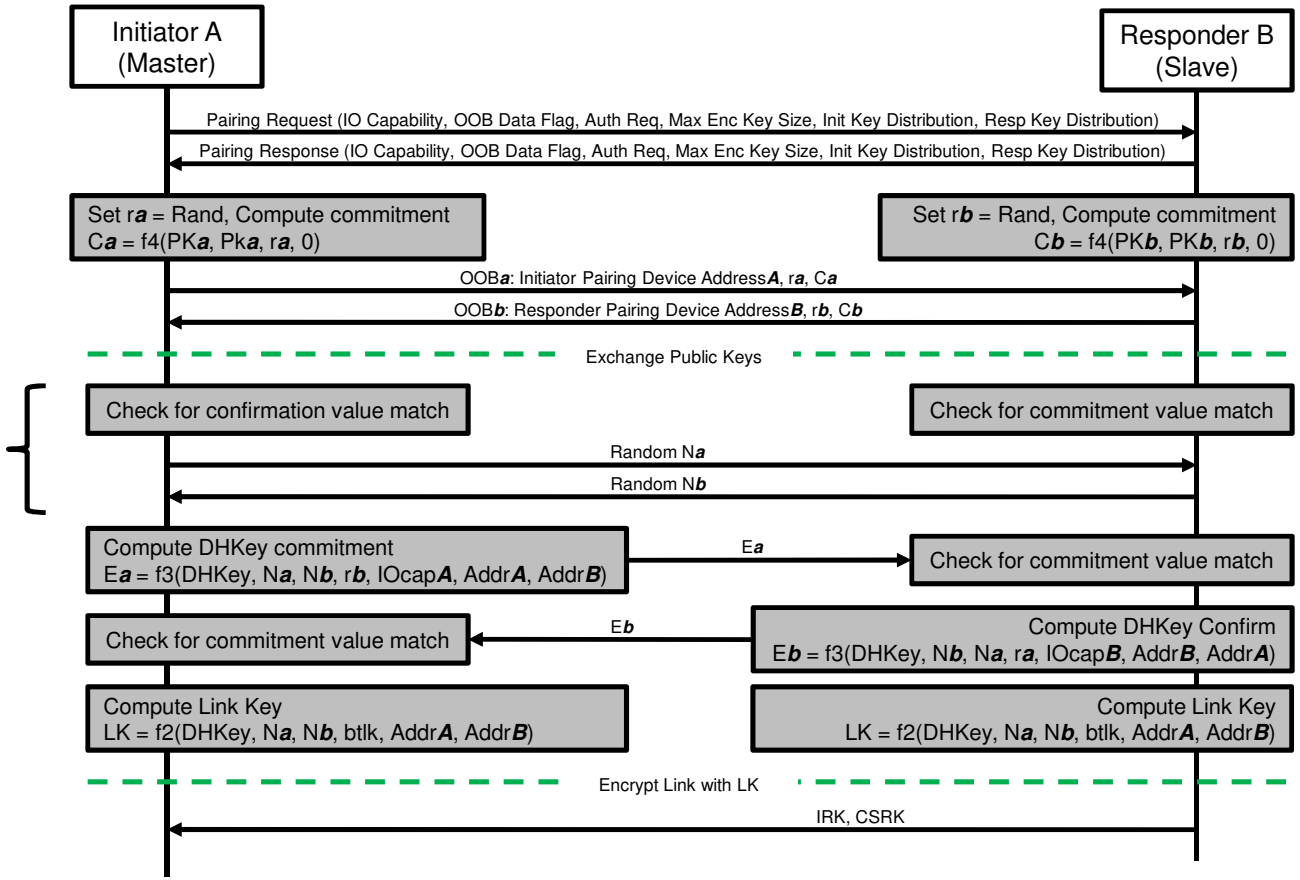
OOB LE Secure Pairing Process

Dynamic Handover

Phase 2: Key Agreement

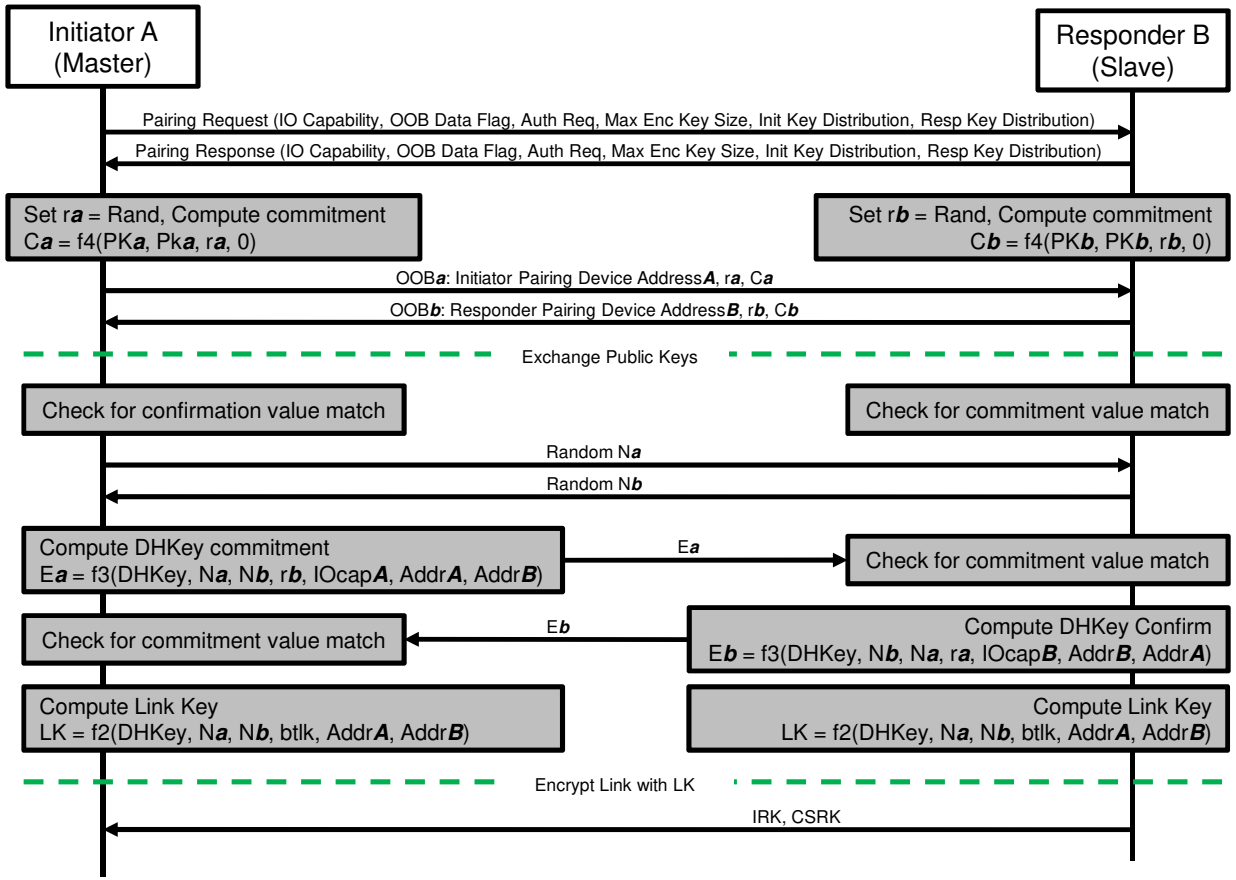
Step 3: The slave re-computes the master's commitment and the master re-computes the slave's commitment to see if they match.

If they do, the master and slave exchange random numbers that will be used to verify the Diffie Hellman Key.



OOB LE Secure Pairing Process

Dynamic Handover



Phase 2: Key Agreement

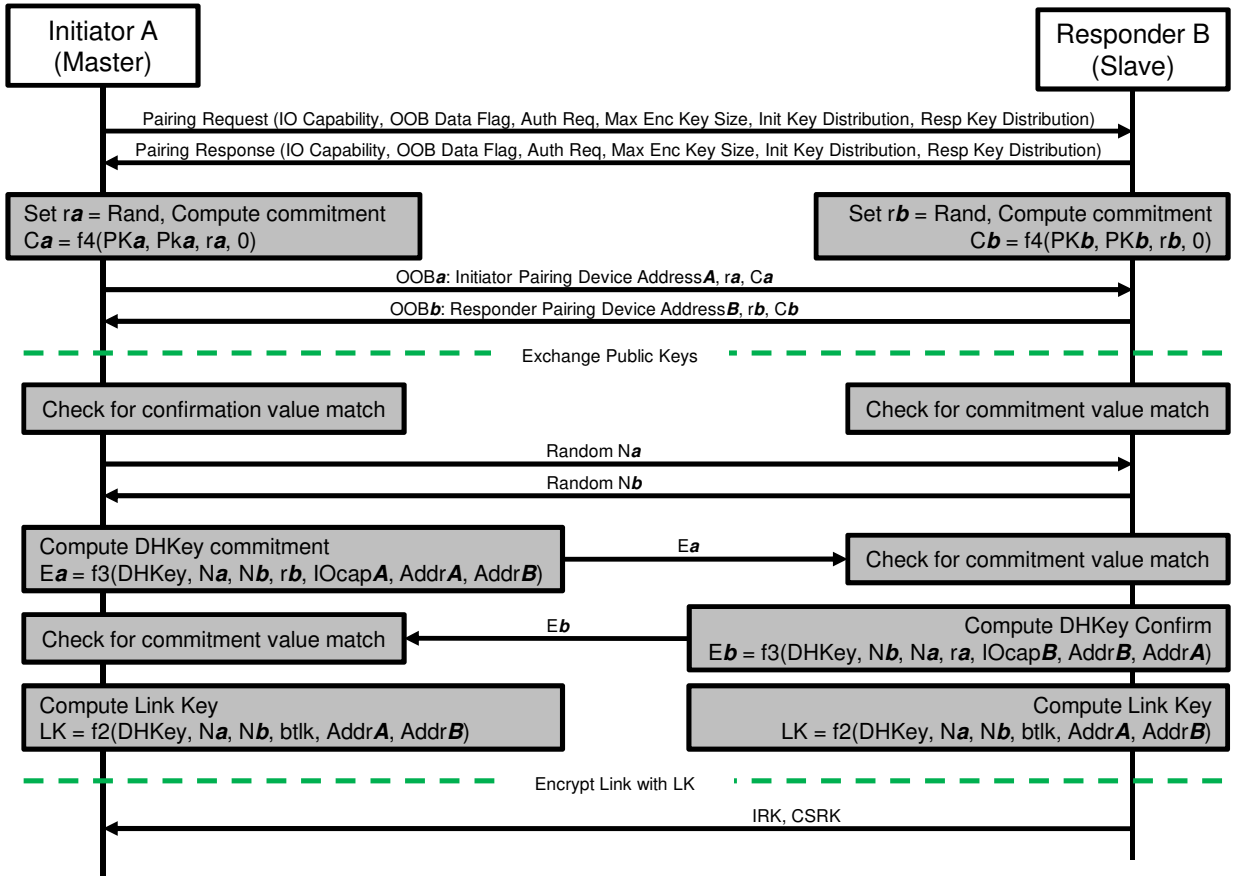
Step 4: The master computes its DHKey commitment and sends that to the slave.

The slave verifies the master's DHKey commitment and, if successful, the slave computes its commitment and forwards that to the master. The master then verifies the slave's DHKey commitment.

life.augmented

OOB LE Secure Pairing Process

Dynamic Handover



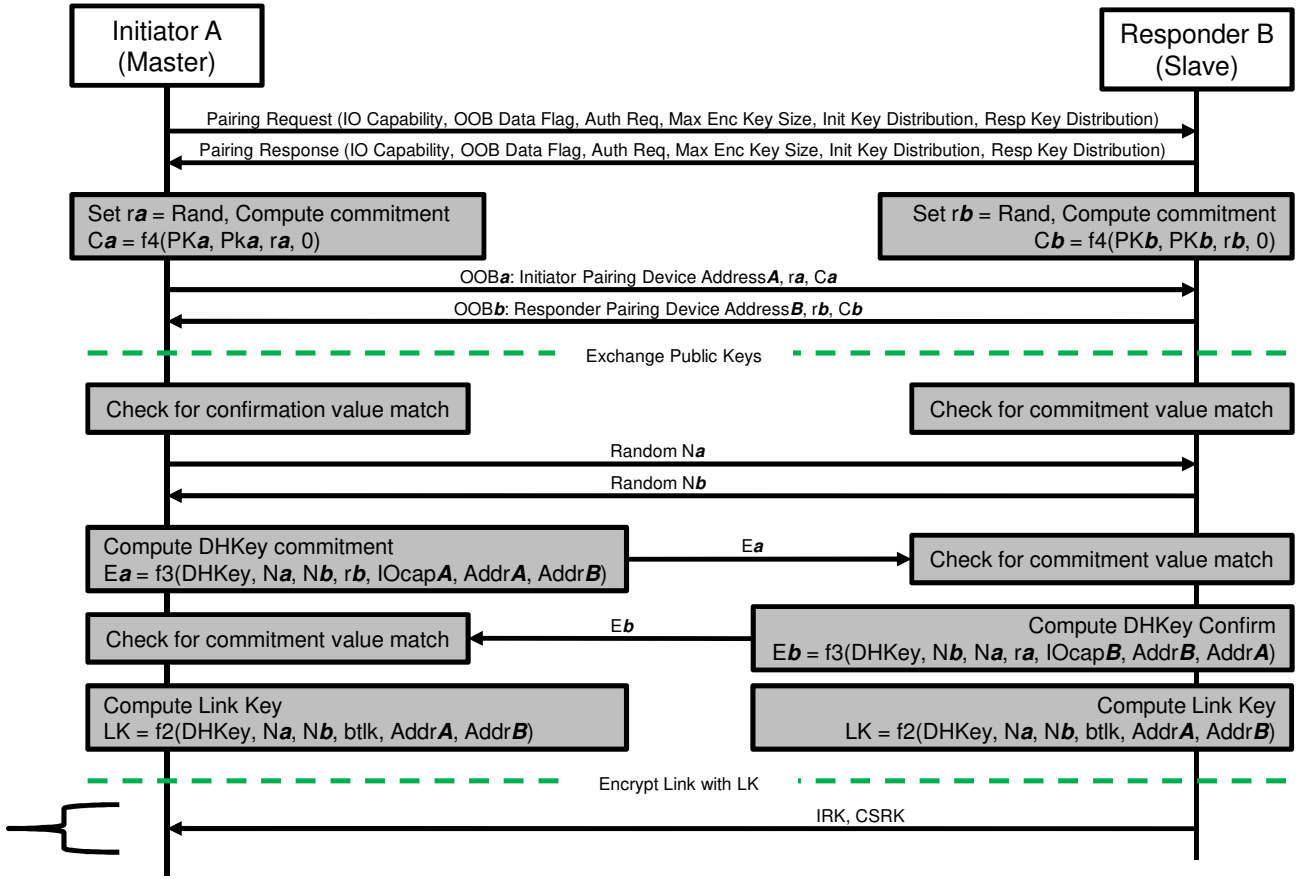
Phase 2: Key Agreement

Step 5: If the master and slave verifies each other's DHKey commitment then they both compute the same Link Key used to symmetrically encrypt the link

life.augmented

OOB LE Secure Pairing Process

Dynamic Handover



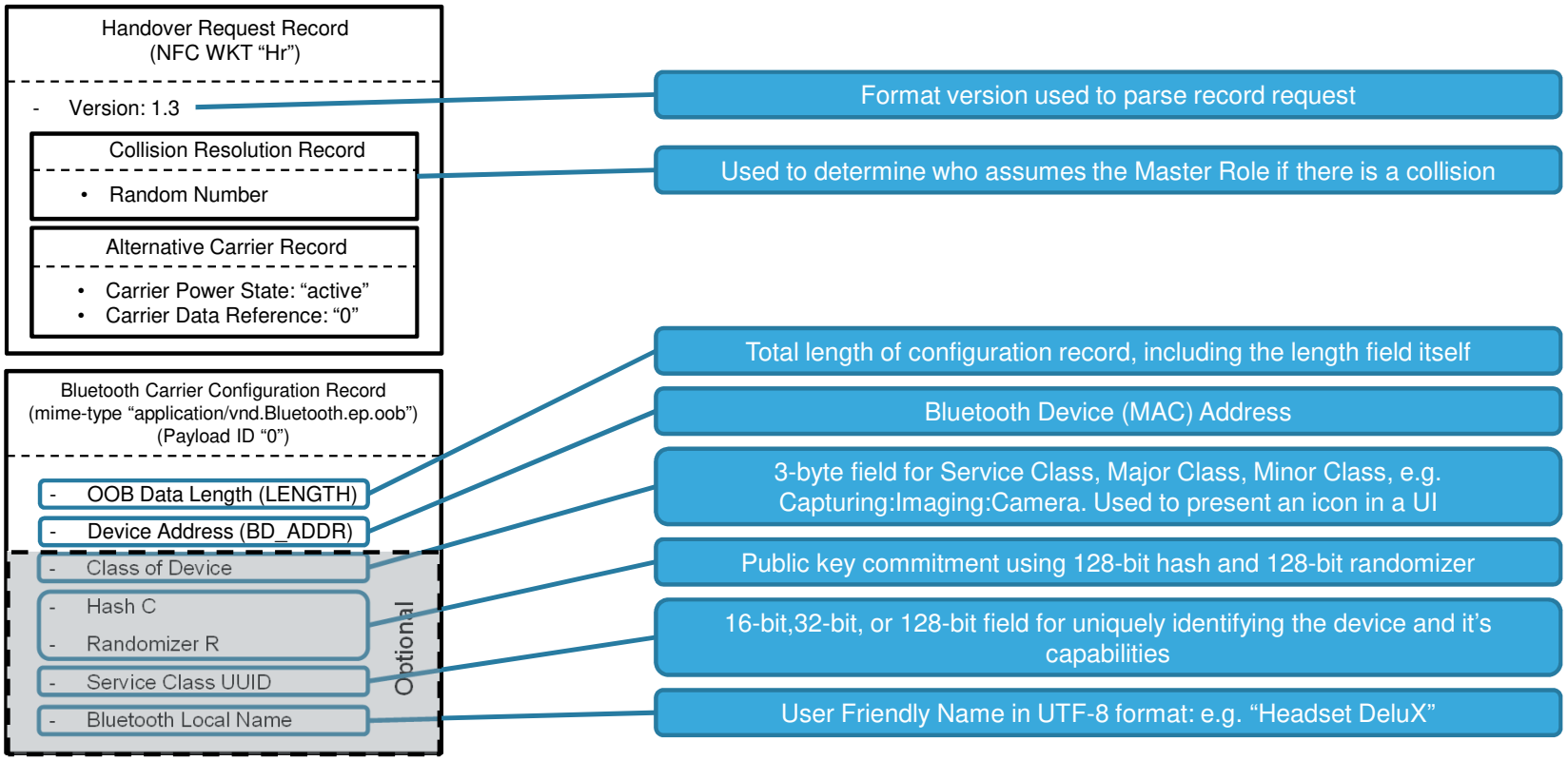
Phase 3: Key Distribution

Once the link is encrypted with the Link Key, the Identity Resolving and Connection Signature Resolving Key can be distributed

life.augmented

Handover Request Record

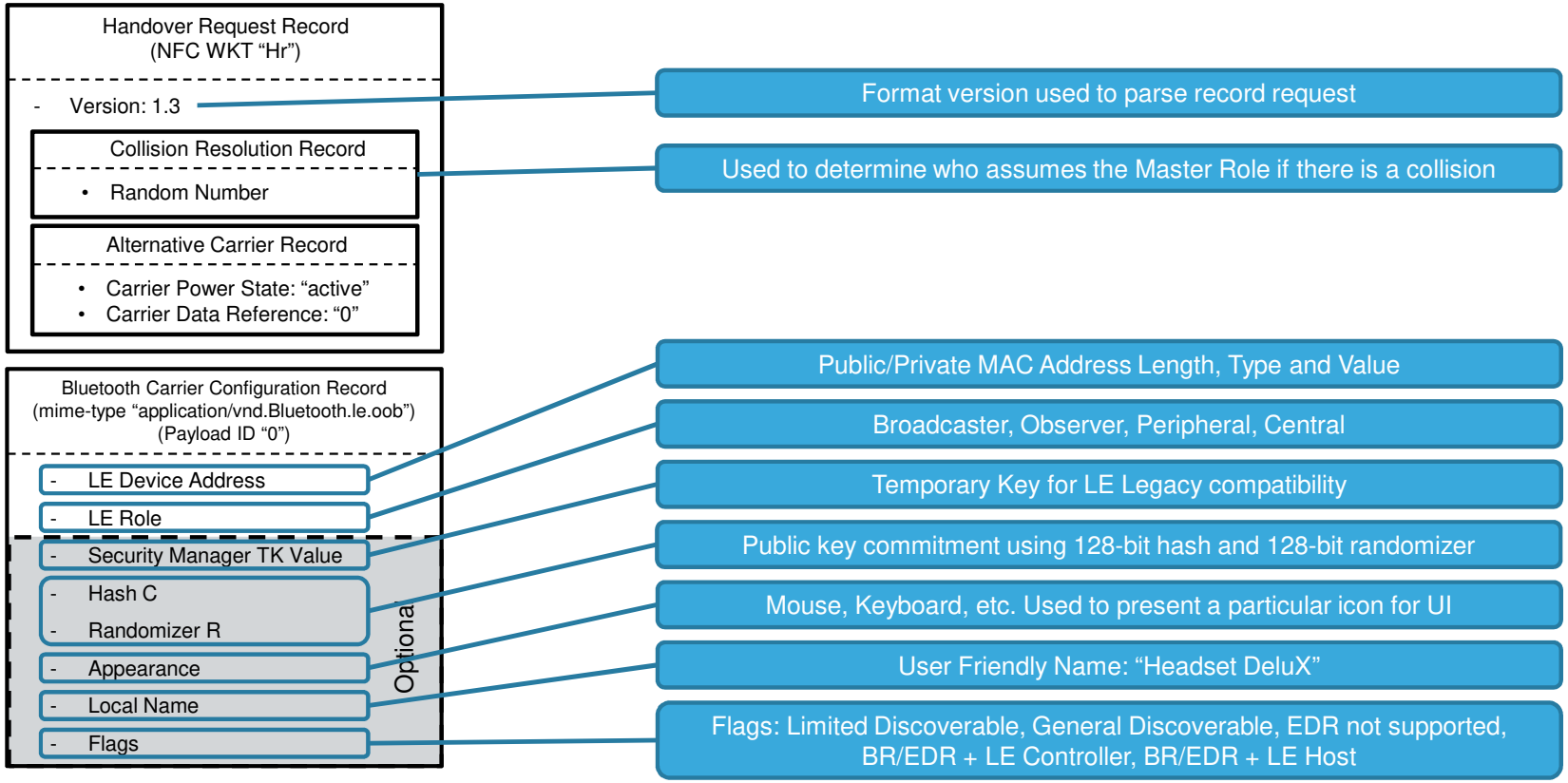
Bluetooth BR/EDR



life.augmented

Handover Request Record

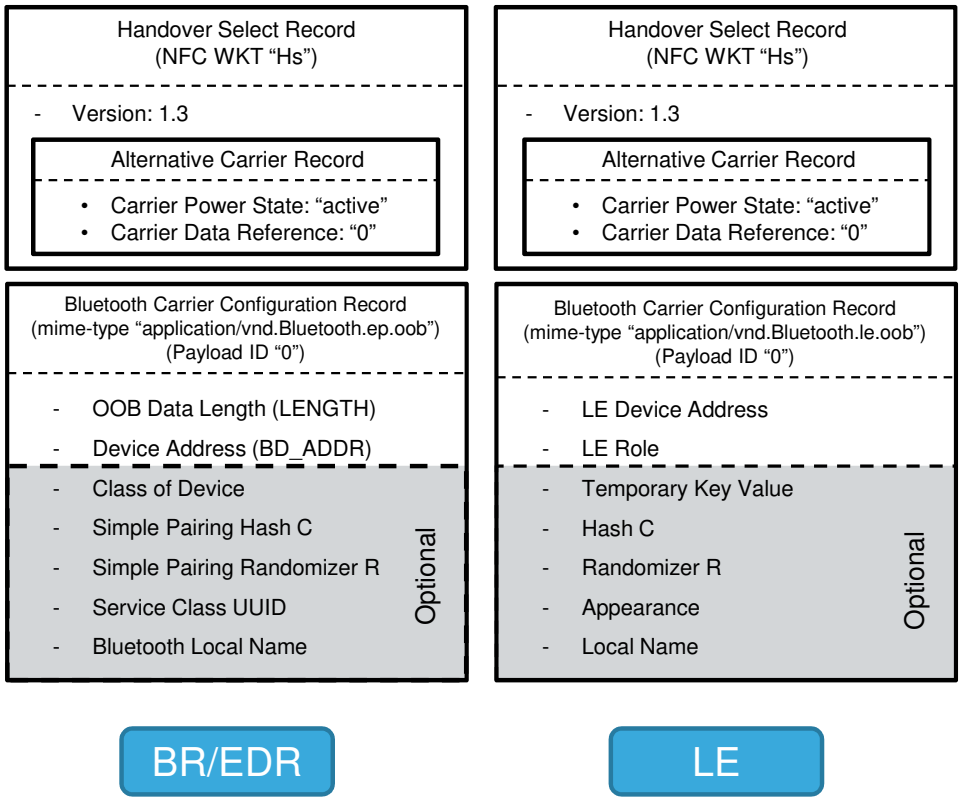
Bluetooth LE



Handover Select Record

Negotiated Handover – NFC Transceiver

- A responder with a NFC transceiver is able to actively negotiate a pairing with an initiator. It can selectively advertise certain capabilities (carriers) while hiding others.
- Mutual Authentication is supported by exchanging Commitments and Randomizers. These can also be changed on every pairing to improve security.
- Role conflicts with the Initiator can be resolved if the Selector changes it role.
- A dynamic tag (e.g. ST25DV) can support negotiated handovers with NFC transceiver in reader mode.

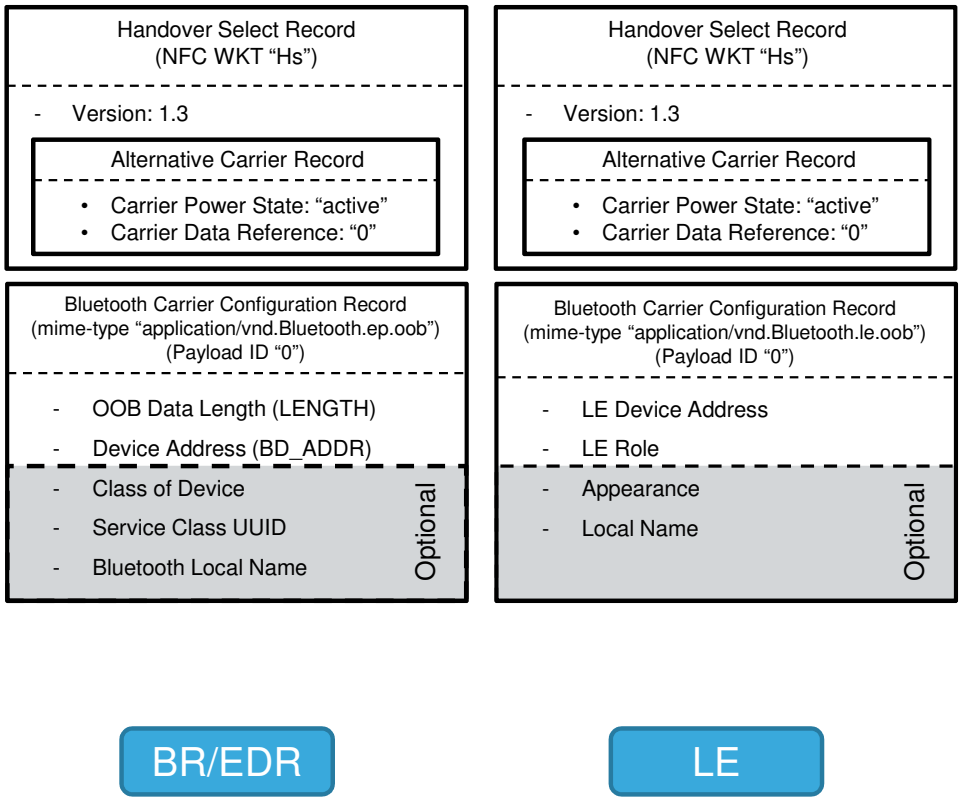


life.augmented

Handover Select Record

Static Handover – NFC Tag

- The Handover Select Message stored on a static NFC Forum Tag is a simplified version of a Handover Select Message returned by an active NFC Forum Device.
- All available carriers will be advertised since the tag has no connection to the Bluetooth radio
- Since data stored on an static tag cannot be changed, the TK value, the Secure Connections Randomizer and Confirmation values are removed and a static private address is used.



ST25 products and demos

life.augmented

ST NFC/RFID Frontend Portfolio

	ST25R95*	ST25R3912/13	ST25R3911B	ST25R3916
Description	Entry-Level Reader	Mid-Range Reader & NFC initiator	High-Perf Reader & NFC Frontend	Ultimate NFC Frontend
Reader/Writer mode	ISO14443A/B ISO15693 Felica	ISO14443A/B ISO15693 FeliCa	ISO14443A/B ISO15693 FeliCa	ISO14443A/B ISO15693 FeliCa
Card emulation mode	Yes (optional)	-	-	Yes
P2P mode	-	Yes	Yes	Yes
RF speed	848kbps	848kbps	6.8Mbps (VHBR)	848kbps
Market certification	-	Payment (EMVco, PBOC, mini-pay)	Payment (EMVco, PBOC, mini-pay)	Payment (EMVco, PBOC, mini-pay)
Advanced features	Inductive wake-up	AAT (3913 only), DPO, Inductive wake-up	AAT, DPO, Cap & Ind wake-up	2DAAT, DPO, Cap & Ind wake-up
HW Interface	SPI 2Mbps, UART	SPI 6Mbps	SPI 6Mbps	SPI 6Mbps
SW Interface	RFAL Unified Software Library for Frontends			
Power supply	2.7V - 5.5V	2.4V – 5.5V	2.4V – 5.5V	2.4V – 5.5V
Output power	0.23W	1.0W	1.4W	1.6W
Temperature range	-25°C to +85°C	-40°C to +125°C	-40°C to +125°C	-40°C to +125°C
Package	QFN32 (5x5 mm)	QFN32 (5x5 mm) / WLCSP (3912 only)	QFN32 (5x5 mm) / Wafer	QFN32 (5x5 mm) / WF /WLCSP

VHBR: Very High Baud Rate
P2P: Peer to Peer mode
AAT: Automatic Antenna Tuning
AWS: Active Wave Shaping

Cap & Ind wake-up: Capacitive & Inductive wake-up
VHBR: Very High Baud Rate
DPO: Dynamic Power Output
DSA: Drive Slope Adjustment

ALM Active Low Modulation
NCI NFC Controller Interface
ANS: Active Noise Suppression

* The ST25R95 and the CR95HF are equivalent

life.augmented

ST25R Series Benefits

- The ST25R family is an integrated reader IC for contactless applications with several benefits:
  - Outstanding analog performance
    - No external amplifier required to achieve high power and long range
    - Automatic antenna tuning (3911B, 3913, 3916)
    - Low power wakeup
    - Excellent P2P interoperability
  - Fast time to market
    - EMVCo, NFC Forum, ISO, and MISRA-C:2012 compliant SW library
    - Single SW library for all products
    - Full integration into STM8 and STM32 eco system
  - Proven solution
    - Market proven solution in the consumer and automotive space
    - Ensures best customer experience

NFC / RFID Tag Product Family

	ST25TB512 ST25TB02K ST25TB04K	ST25TA512B ST25TA02KB ST25TA02KB-D ST25TA02KB-P	ST25TA16K ST25TA64K	ST25TV512 ST25TV02K ST25TV02K-AD	ST25TV64K
Contactless Interface	ISO14443B	ISO14443A NFC Forum Type 4	ISO14443A NFC Forum Type 4	ISO15693 NFC Forum Type 5	ISO15693 NFC Forum Type 5
RF range	Short range (up to 10cm)	Short range (up to 10cm)	Short range (up to 10cm)	Long range (up to 100cm)	Long range (up to 100cm)
RF speed	106kbps	106kbps	106kbps	26kbps (53kbps)	26kbps (53kbps)
Memory format	EEPROM data	EEPROM (preformatted NDEF)	EEPROM (preformatted NDEF)	EEPROM (preformatted NDEF)	EEPROM data
Memory size	512-bit & 2k / 4k-bit	512-bit / 2k-bit	16k / 64k-bit	512-bit / 2k-bit	64k-bit
Data protection	OTP bits	Password 128-bit Digital signature	Password 128-bit	Password 64-bit Digital signature	Password 32-bit
Digital output	NA	GPO Field detect -P: CMOS_P -D: Open-drain	NA	Tamper Detect	NA
Counter	32-bit (x2)	20-bit	NA	16-bit	NA
RF tuning capacitor	64pF	50pF	25pF	23.5pF & 97pF	28.5pF
Temperature range	-40°C to +85°C	-40°C to +85°C	-40°C to +85°C	-40°C to +85°C	-40°C to +85°C
Package	SBN12 *	SBN12 * / SBN075 ² FPN5 (1.7x1.4mm)	SBN12 *	SBN12 * / SBN075 ²	SBN12 *

* SBN12: Die form, sawn and Bumped wafer, 120µm thickness, inkless 8” wafer
² SBN075: Die form, sawn and Bumped wafer, 75µm thickness, inkless 8” wafer

NFC / RFID Dynamic Tag Family

	M24SR02 M24SR04 M24SR16 M24SR64	ST25DV04K ST25DV16K ST25DV64K
Contactless Interface	ISO14443A NFC Forum Type 4	ISO15693 NFC Forum Type 5
RF range	Short range (up to 10cm)	Long range (up to 100cm)
RF speed	106kbps	26kbps (53kbps Fast Read)
Memory format	EEPROM (preformatted NDEF)	EEPROM
Memory size	2k-bit / 64k-bit	4k-bit / 64k-bit
Data protection	Password 128-bit	Password 64-bit
Digital output	GPO Field detect (Open Drain)	GPO Field detect (Open Drain or CMOS)
Serial Interface	I^2C @ 1MHz	I^2C @ 1MHz
Fast Transfer Mode	No	Yes (256 byte SRAM buffer)
Energy Harvesting	No	Yes
Additional Features	RF Disable	RF Disable / Sleep / Low Power Down
RF tuning capacitor	25pF	28.5pF
Temperature range	-40°C to +85°C (RF)	-40°C to +105°C (RF)
Package	SO8 / TSSOP8 / UFDFPN8 SG121 Wafer	SO8 / TSSOP8 / UFDFPN12 (all) UFDFPN12 / WLCSP10 / Wafer (04K only)

ST25DV-I2C Evaluation Boards

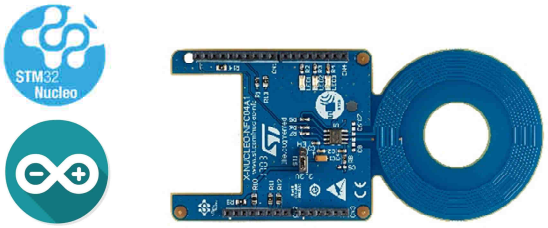
ST25DV-I2C discovery kit

- **ST25DV04K** Dynamic NFC tag IC
- 40x24mm 10 turns antenna (ANT Class5)
- STM32F405 MCU
- 2.4” TFT LCD Touch screen
- I2C & SWIP connectors
- Daughter board connector

ST25DV-DISCOVERY

ST25DV-I2C Nucleo shield

- **ST25DV04K** Dynamic NFC tag IC
- Ø54mm 8 turns single layer antenna etched
- Energy harvesting, Low Power mode, GPO
- Compatible with STM32 Nucleo boards
- I2C interface to MCU & Powered through Arduino™ connector



X-NUCLEO-NFC04A1

ST25DV-I2C Antenna kit

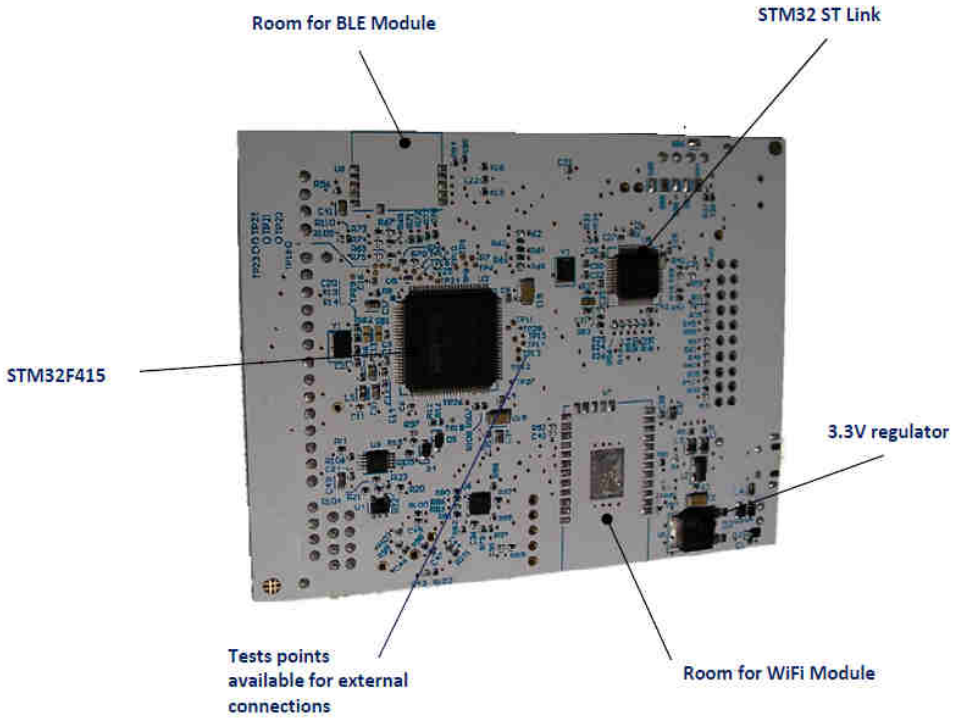
- **ST25DV04K** Dynamic NFC tag IC
- Ready-to-use PCB including:
- 45x75mm (ST25DV_Discovery_ANT_C1)
- 18x24 mm (ST25DV_Discovery_ANT_C6)
- Energy Harvesting output (Vout)
- Mates with ST25Dx_Discovery MBoard

ANT-1-6-ST25DV

life.augmented

Bluetooth Modules

For ST25DV-Discovery Board



BluNRG-M0
BT v4.2 Module

BluNRG-M2
BT v5.0 Module

life.augmented

CR95HF*/ST25R95 Evaluation Boards

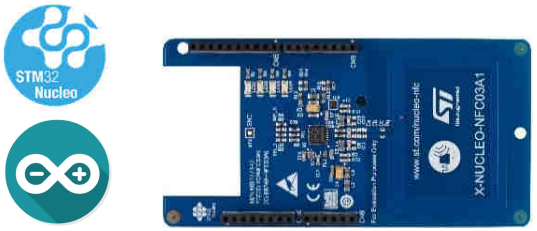
CR95HF demo board

- **CR95HF** NFC multi-protocol reader IC
- 47x34 mm 2 turns double layer antenna etched on PCB and associated tuning circuit
- STM32F1 micro-controller
- USB & JTAG connectors

M24LR-DISCOVERY KIT

ST25R95 Nucleo shield

- **ST25R95** NFC multi-protocol reader IC
- 47x34mm 4 turns antenna etched on PCB
- SPI (Slave interface) or UART
- Up to 528-byte command/reception buffer
- Optimized power management
- Powered through Arduino™ UNO R3 connector



X-NUCLEO-NFC03A1

* The ST25R95 and the CR95HF are equivalent

ST25R3911B Evaluation Boards

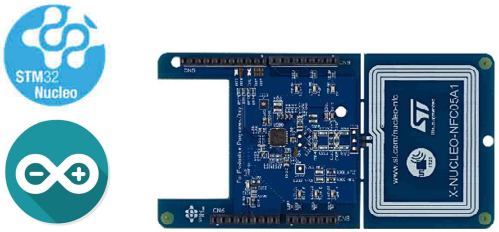
ST25R3911B discovery kit

- **ST25R3911B** HF reader / NFC initiator IC
- 105x52mm 2 turns antenna and associated VHBR tuning circuit
- STM32L476RET6 32-bit MCU
- Micro-USB connector
- Additional UART / I²C Host interfaces, as well as NFC SPI and JTAG/SWD points

ST25R3911B-DISCO

ST25R3911B Nucleo shield board

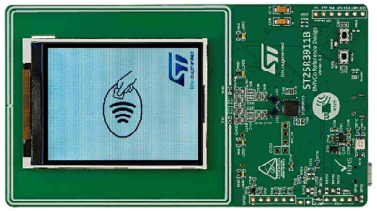
- **ST25R3911B** HF reader / NFC initiator IC
- 47x34mm 4 turns antenna
- Compatible with STM32 Nucleo boards
- Equipped with Arduino™ UNO R3 connector



X-NUCLEO-NFC05A1

ST25R3911B EMVCo Demo kit

- **ST25R3911B** HF reader / NFC initiator IC
- 65x74mm 2 turns antenna etched on PCB
- STM32L476 32-bit MCU
- Micro-USB connector
- Comprehensive Device Test Environment (DTE) for EMVCo Level 1 FW control
- S-Touch controller



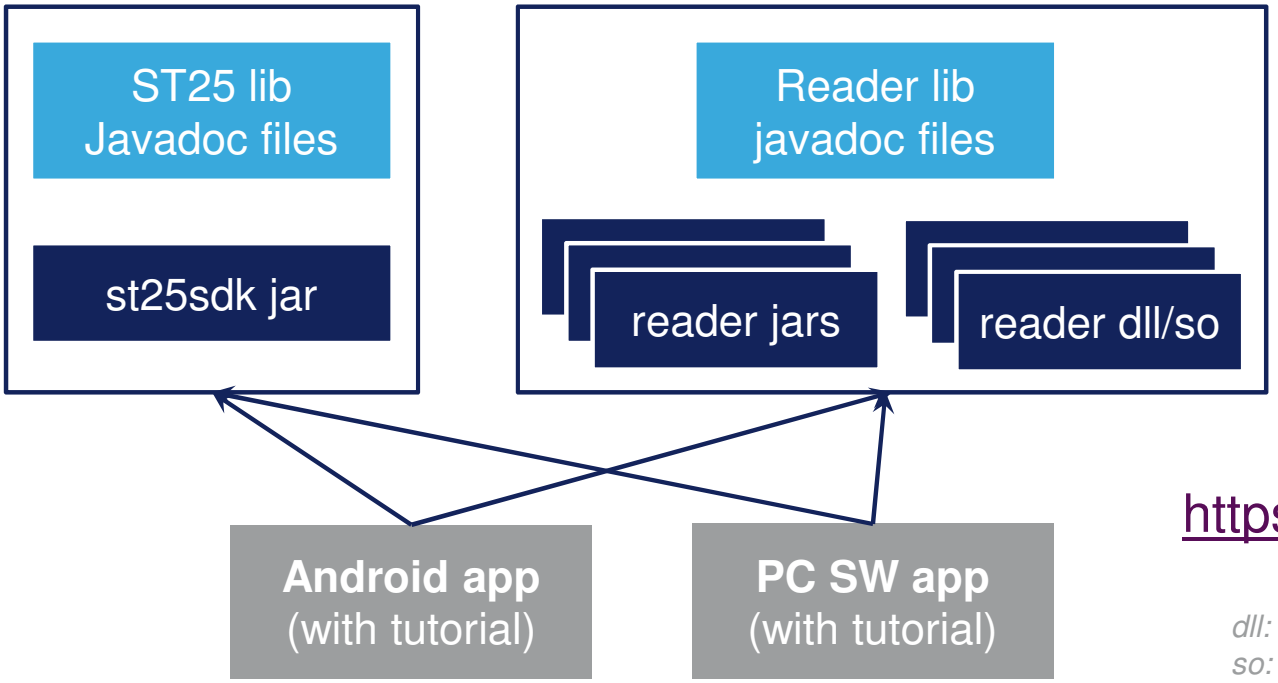
ST25R3911B-EMVCO

life.augmented

ST25R3911B discovery kit and Nucleo shield are also valid for ST25R3912, ST25R3913, ST25R3914 and ST25R3915

ST25 Software Development Kit

Create your own NFC JAVA application

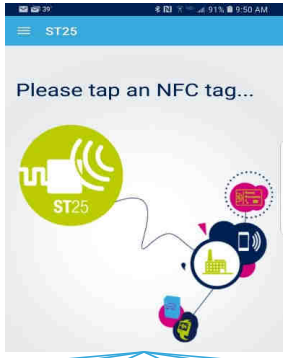


https://www.st.com/st25sdk

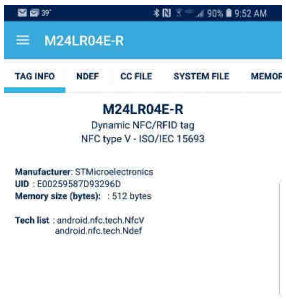
dll: dynamic link library (for Windows)
so: shared object (dynamic library for Linux)

life.augmented

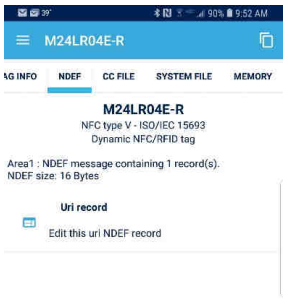
Android Tap App



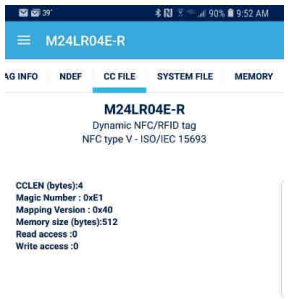
Tag Info



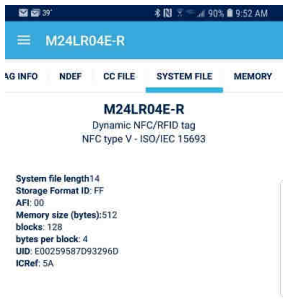
NDEF



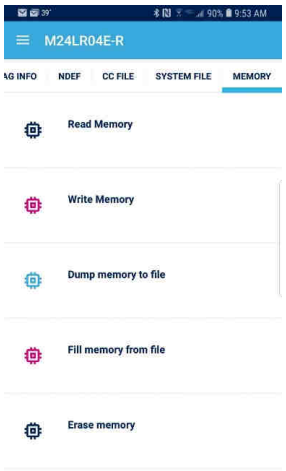
CC File



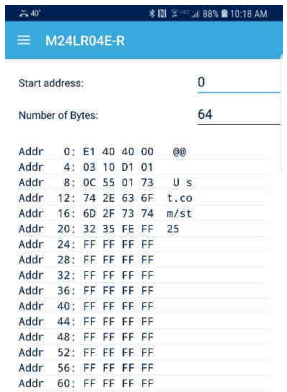
System File



Memory

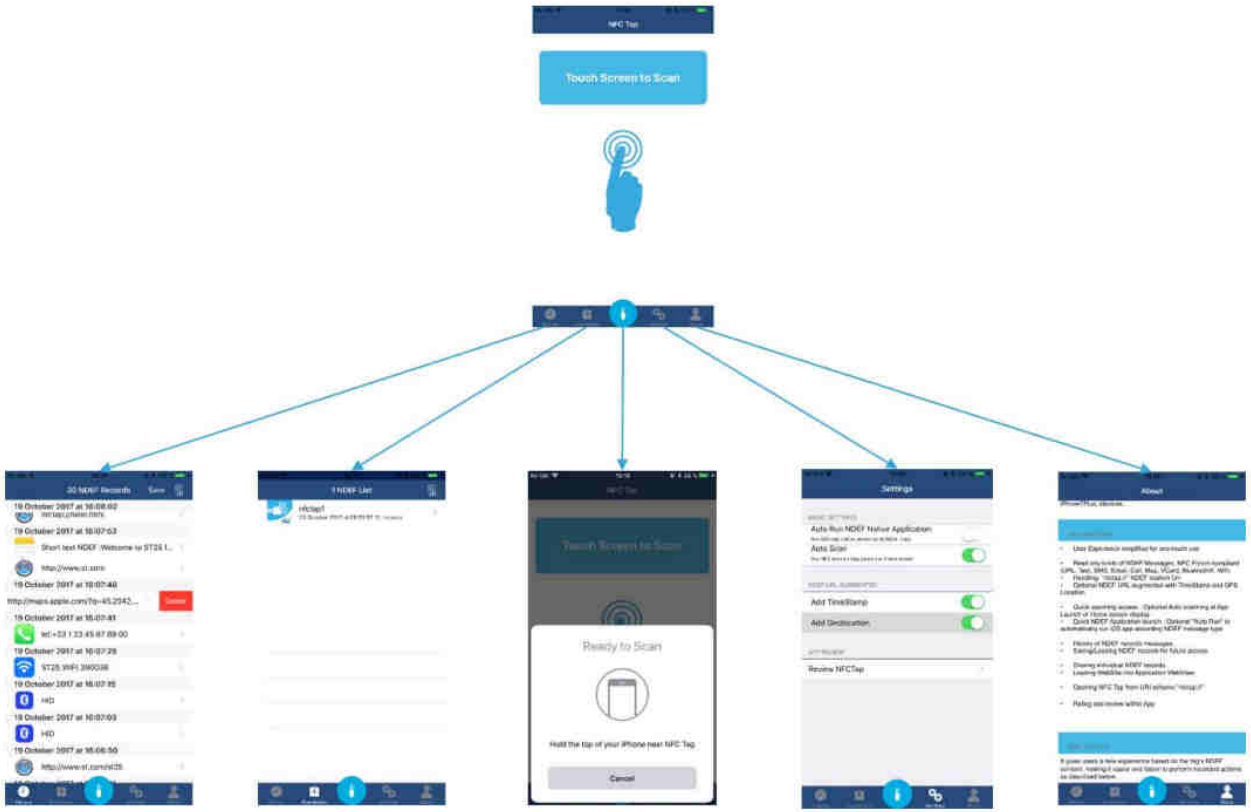


Contents



life.augmented

iOS Tap App



life.augmented

ST25 Simply More Connected

Thank You!