CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique

CRT centre de ressources technologiques

Journée sur la sécurité des piles réseaux
(Journée commune au GDR RSD, GPL (GT GLSEC) et SI (GT SSLR))

La sécurité dans le Bluetooth Low Energy

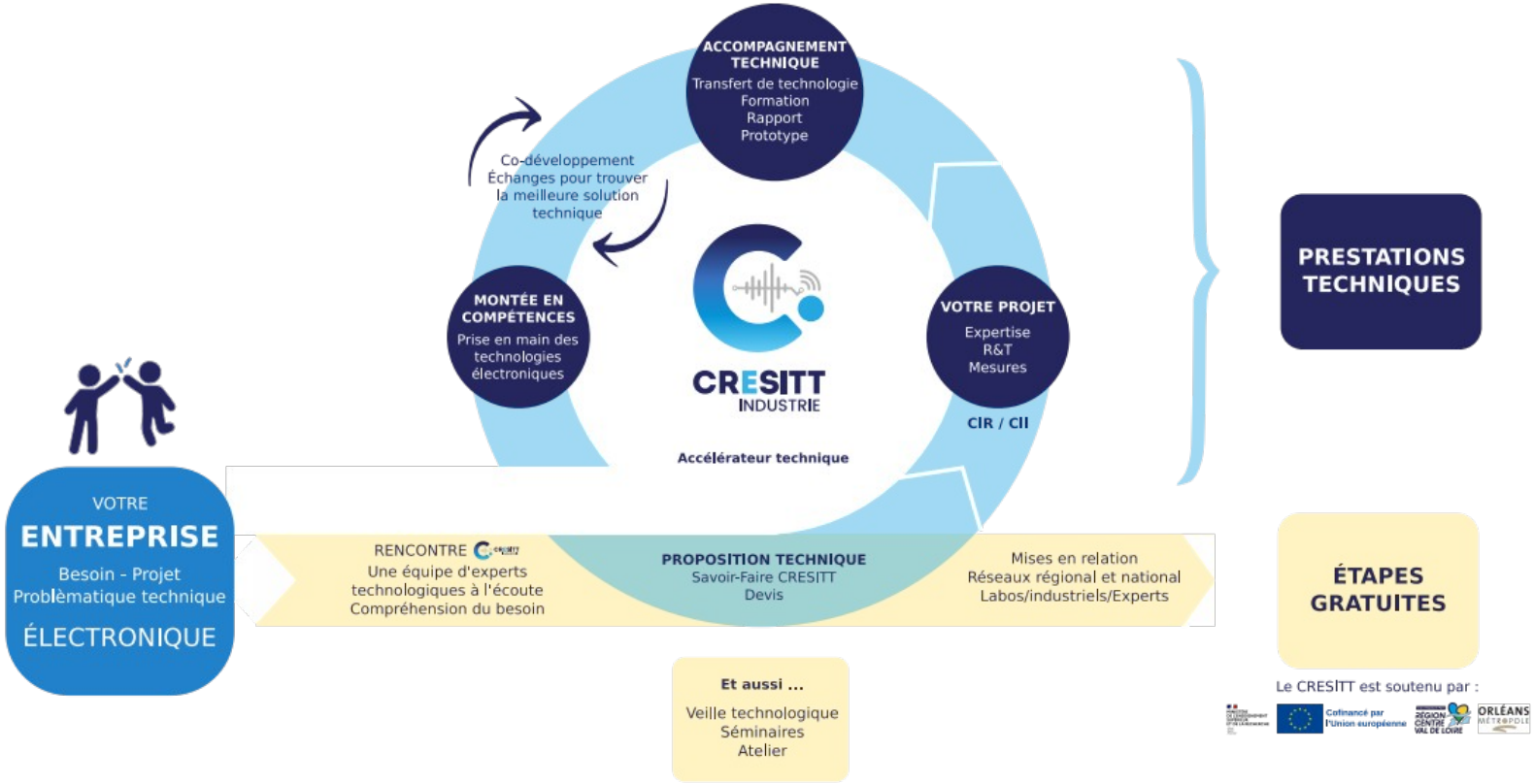
Le CRT CRESITT est soutenu par :

Ministère de l'Enseignement supérieur et de la Recherche
Cofinancé par l'Union européenne
Région Centre Val de Loire
Orléans Métropole

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

© CRESITT Industrie – FE01 11 IndH

TECHNOLOGIES ÉLECTRONIQUES



© CRESITT Industrie 2024

Compétences CRESITT :
Du capteur au transfert de données sécurisé

HARDWARE

Capteurs et mise en forme des signaux

Électronique analogique & numérique

Analog front end

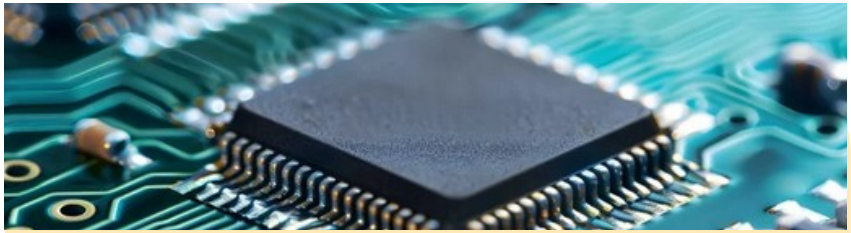
Architectures dédiées à l'embarqué, dont µcontrôleurs et FPGA

Systèmes d'alimentation

Convertisseurs d'énergie DC/DC

Optimisation électronique de puissance

Adaptation et Design d'antenne



FIRMWARE

Acquisition et processing

Traitement des signaux embarqués

Logiciels couches basses embarqués

Sécurisation

Protocoles sans fils :
BLE, LORA, Matter, RFID UHF, NFC,...

Gestion de l'énergie

Linux embarqué

Protocoles réseaux : MQTT , HTTPS, …

OPTIMISATION DES PERFORMANCES RF ET ÉNERGÉTIQUE

© CRESITT Industrie 2024

Compétences CRESITT :
Instrumentation / Mesures

COMPATIBILITÉ ELECTRO-MAGNÉTIQUE

Rayonnée et Conduite

Immunité et Emissivité

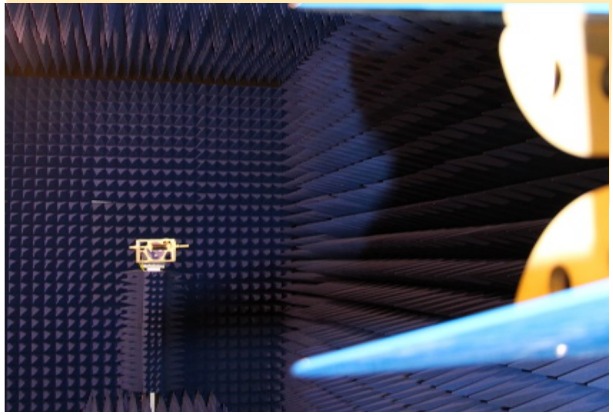
Marquage CE

RADIOFRÉQUENCES

Choix, adaptation et mesures d'antennes

Mesures selon directive RED

Simulations de propagations et conception d'antennes



SYSTÈMES AUTONOMES

Mesures de consommations électriques

Gestion des différentes sources d'alimentation et techniques de récupération d'énergie

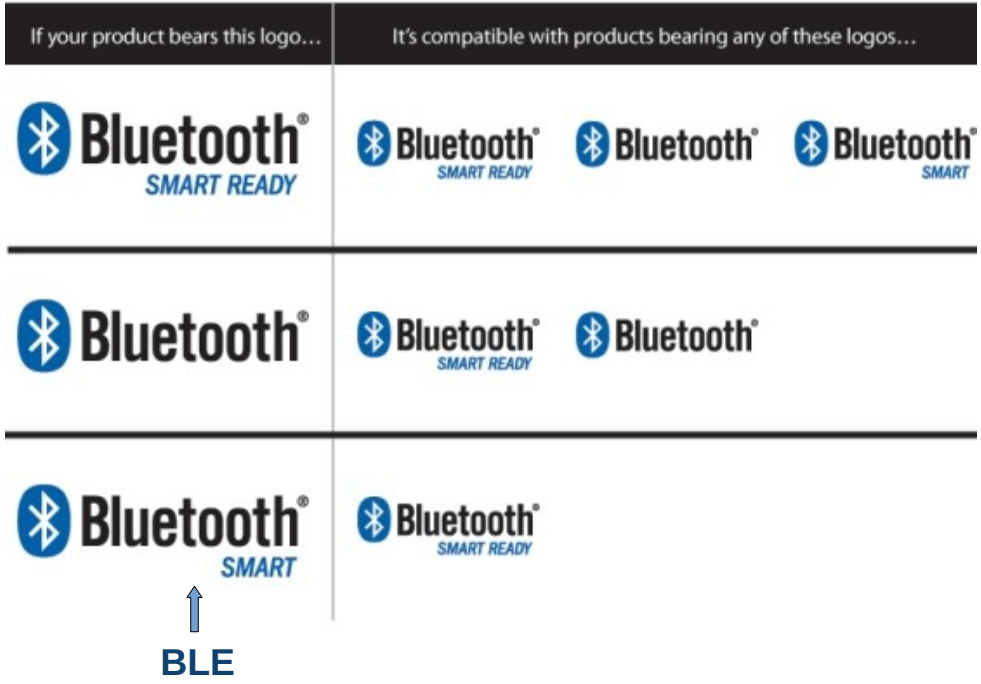
© CRESITT Industrie 2024

SOMMAIRE

- Présentation Bluetooth, Smart et Smart Ready
- Le Bluetooth Low Energy (BLE)
  - Technologie
  - Protocole
  - Sécurité
  - Vulnérabilités

© CRESITT Industrie 2024

Bluetooth & BLE



© CRESITT Industrie 2024

Bluetooth & BLE

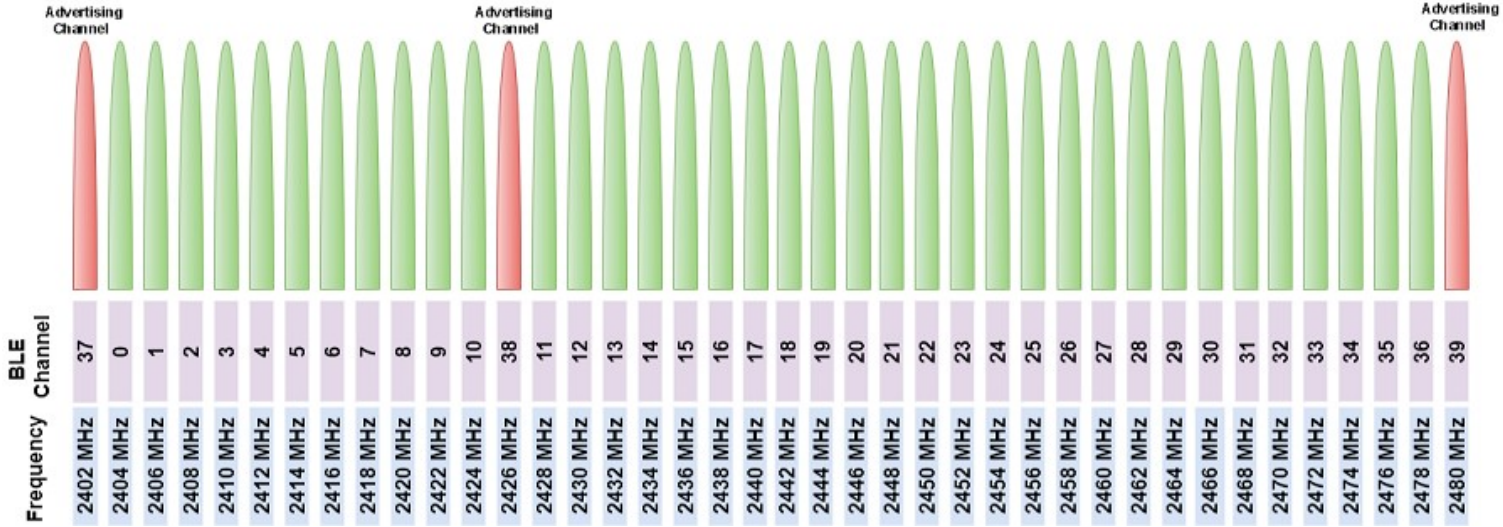
bande ISM des 2.4GHz

© CRESITT Industrie 2024

Bluetooth & BLE - Technologie

- Bluetooth et Bluetooth Low Energy
  - Une norme commune actuellement version 5.4
  - Incompatibilité Bluetooth et BLE (couche physique / radio différente)
    - 79 canaux espacés de 1Mhz VS 40 canaux espacés de 2Mhz [2.402GHz – 2.480GHz]
    - 32 canaux pour la découverte VS 3 pour l'advertising
    - 79 canaux pour la connexion VS 37 pour l'échange de données

Bluetooth Low Energy channel (src: mathworks)



© CRESITT Industrie 2024

Bluetooth standard

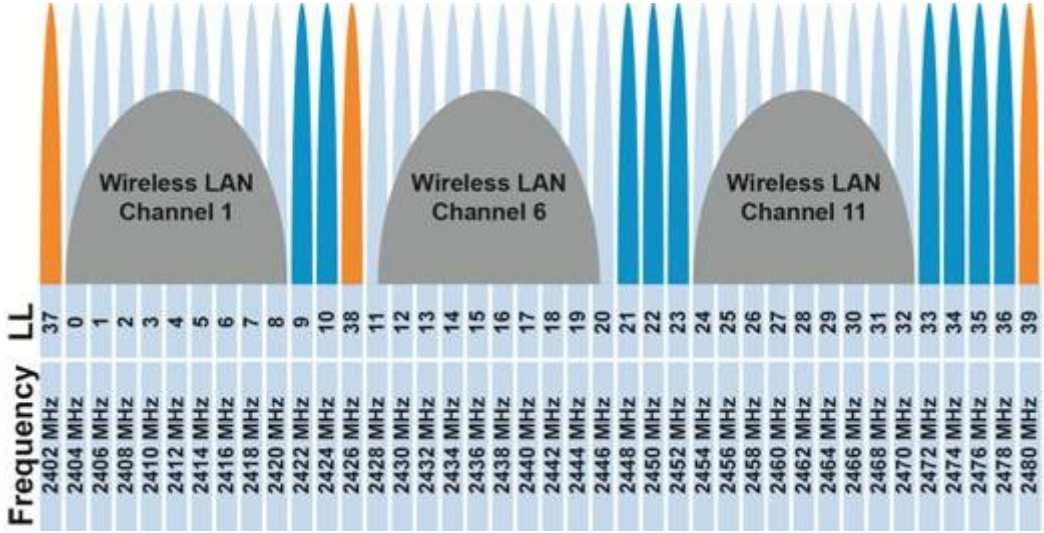
Date	Versions	Utilisation
1998	1ers drafts écrits par Ericsson	
1999	Version 1.0b : BR	Premières oreillettes
2003	Version 1.2 : AFH, extended SCO	Oreillettes avec meilleure qualité audio, souris/clavier sans fils, liaison série sans fils
2004	Version 2.0 : EDR	
2007	Version 2.1 : meilleure sécurité	
2009	Version 3.0 : high Speed	
2010	Version 4.0 : BLE, profile GATT	
2013	Version 4.1 :	
2014	Version 4.2 : LE Secure Connections	
2017	Version 5.0 : 2Mbit/s	Réseau Mesh, advertising étendu
2019	Version 5.1 : Le Isochronous channel	Amélioration de la portée, localisation
2020	Version 5.2 : Le power control	Broadcast audio avec un nombre illimité d'utilisateurs
2022	Version 5.3 : Conso plus faible, contrôle de la taille de clef de chiffrement	
2023	Version 5.4 : Ajout characteristic LE GATT Security Levels, chiffrement advertising, Periodic Advertising with Responses (PawR) permet de monter jusqu'à 1650 byte en advertising	
09/2024	Version 6.0	Localisation centimétrique

Historique des utilisations

© CRESITT Industrie 2024

Bluetooth BLE

- Coexistence



© CRESITT Industrie 2024

Bluetooth BLE

- Topologie piconet
  - « en étoile »
  - Le centre du réseau est le maître
  - Les périphériques sont les esclaves
- Réseau BLE
  - Un seul maître
  - Plusieurs esclaves
- Mode radio *Ultra Low Power* du Bluetooth
  - Idle (no Link Layer connection)
  - Connected (At least one LL connection)
- Compatible Bluetooth MESH (>v.5.0)

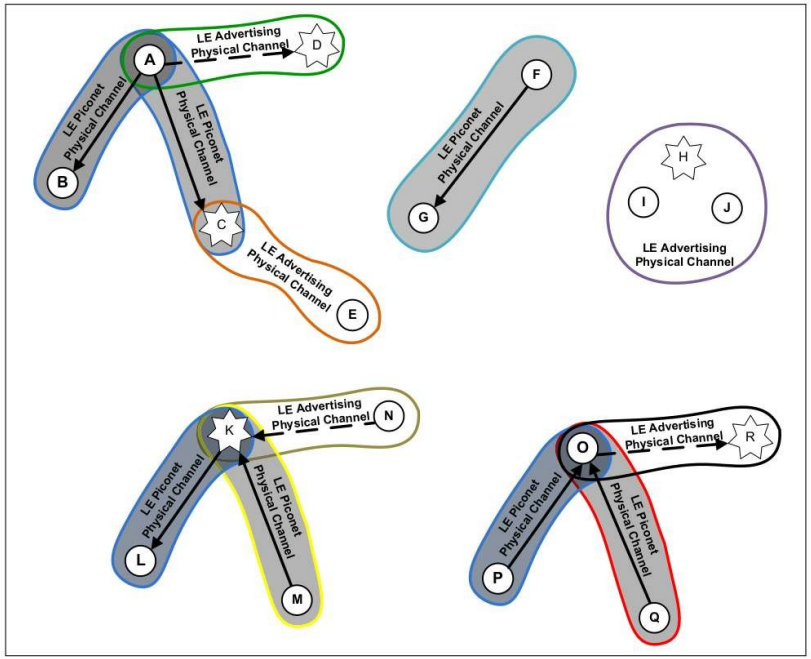


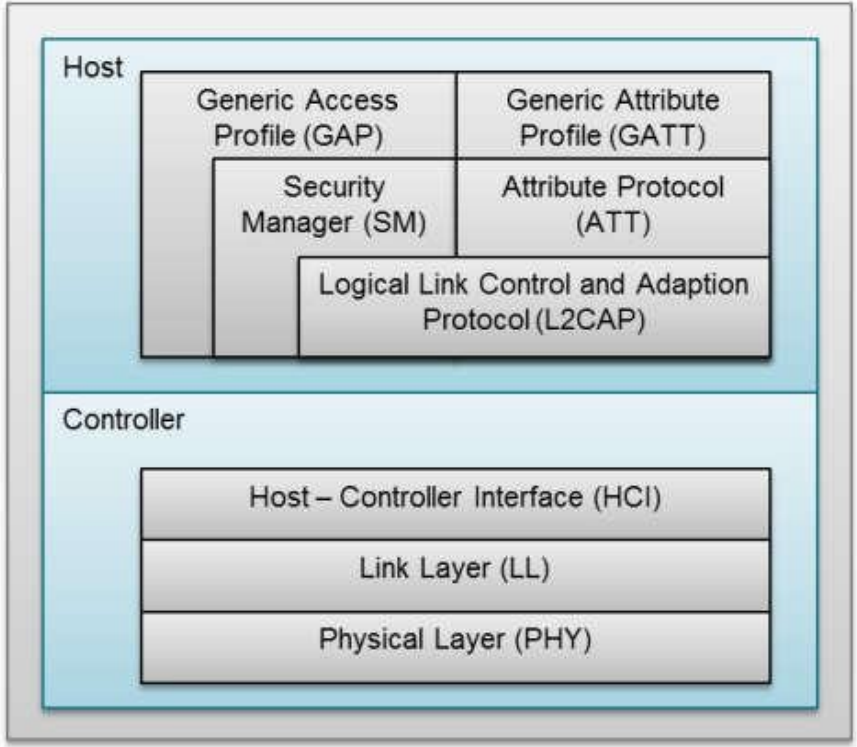
Figure 4.2: Example of Bluetooth LE topology

Devices en advertising sont indiqués avec une étoile
E, I, J : scanner
A, N, O : initiator
F, M, P, Q : central
G, L, O : peripheral

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire *Bluetooth Low Energy*



Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

- *Controller* : plusieurs combinaisons

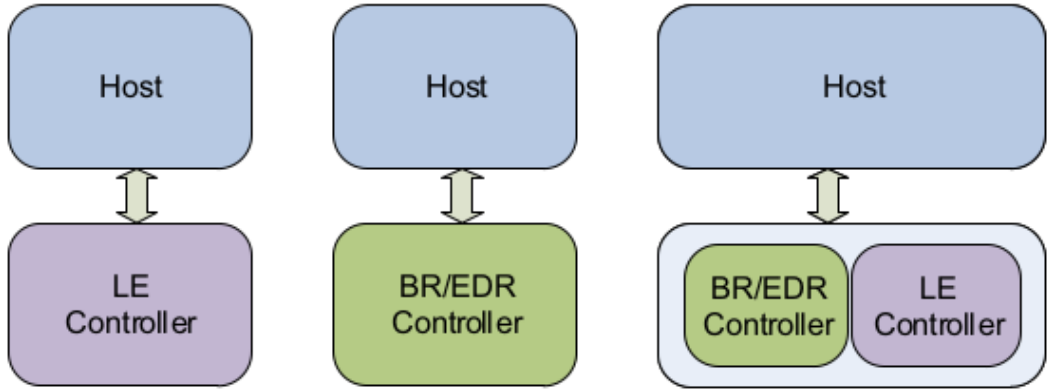


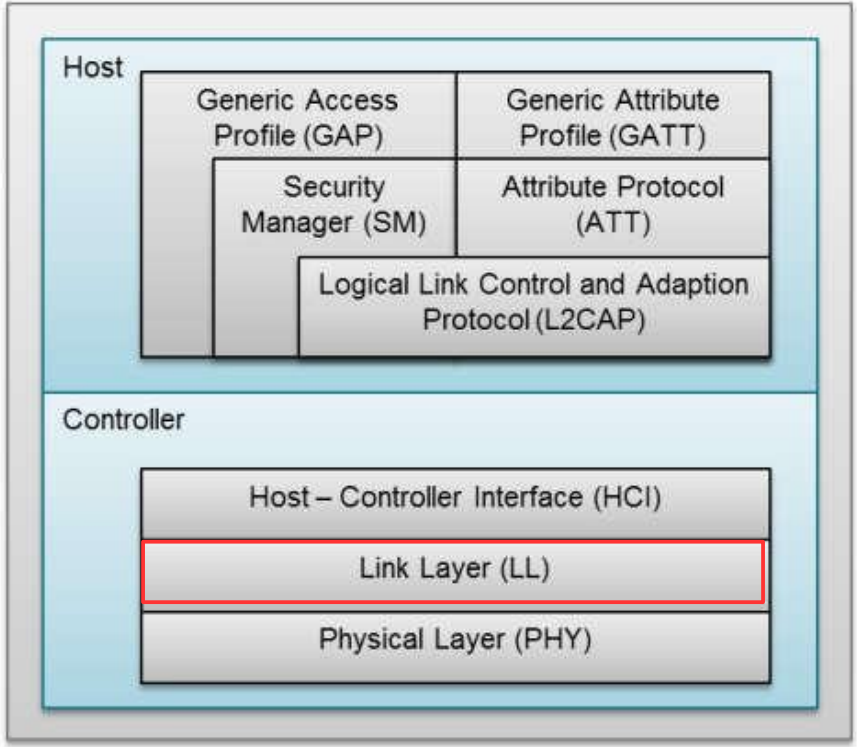
Figure 1.1: Bluetooth Host and Controller combinations: (from left to right): LE Only Controller, BR/EDR only Controller, and BR/EDR/LE Controller

(src: Bluetooth Core specification V5.4)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire *Bluetooth Low Energy*



Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

Link Layer

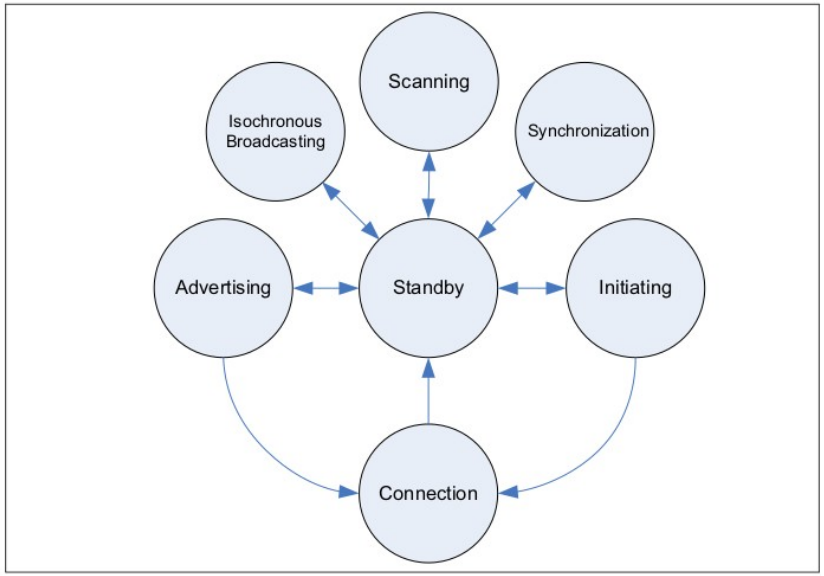


Figure 1.1: State diagram of the Link Layer state machine

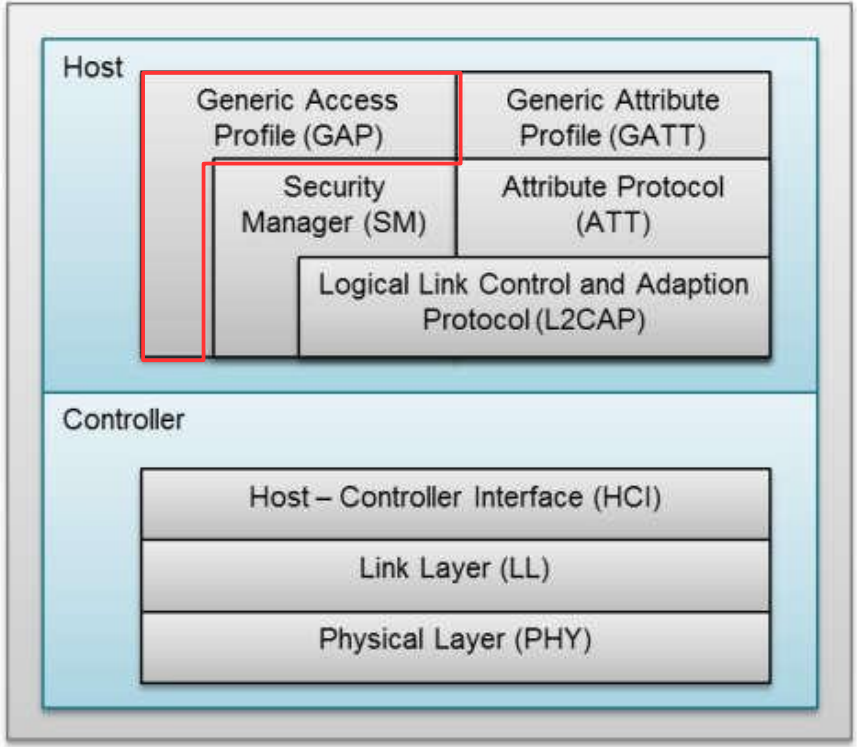
(src: Bluetooth core specification 5.2)

- Gère la machine d'état du système
- Définit les rôles master, slave
- Permet l'activation du chiffrement sur le transport

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire *Bluetooth Low Energy*



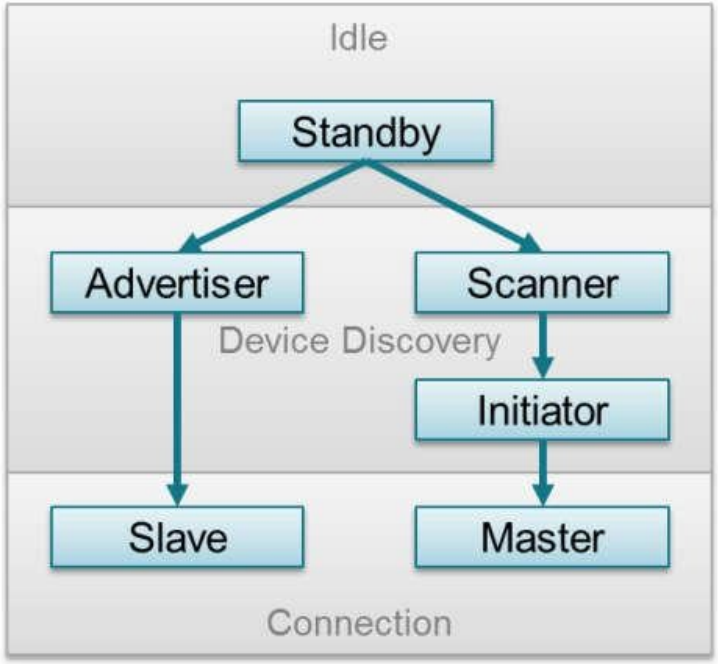
Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

General Access Profile (GAP)



Gap State diagram
(src: texas instrument)

- Couche de gestion des connexions, du niveau de sécurité et de l'*advertising*
  - *Advertiser* : le composant avertit de sa présence et se fait connaître
  - *Scanner* : le composant réagit dès qu'il reçoit un advertising. Il renvoie une requête de scan pour connaître ses possibilités (*service discovery*)
  - *Initiator* : demande de connexion à partir de l'adresse d'un device reçu via l'*advertising*
  - *Master/Slave* :
    SLAVE : lance les *advertising*
    MASTER : scane et initie les connexions

© CRESITT Industrie 2024

- *General Access Profile* (GAP)
  - Gestion des rôles
    - *Broadcaster* : le composant est un advertiser et non connectable (beacon/ibeacon)
    - *Observer* : le composant scan les advertisement mais n'initie pas de connexions
    - *Peripheral* : le composant est un advertiser qui est connectable et deviendra un esclave
    - *Central* : le composant est un scanner qui initiera des connexions.

(src: texas instrument)

Observer

Broadcaster

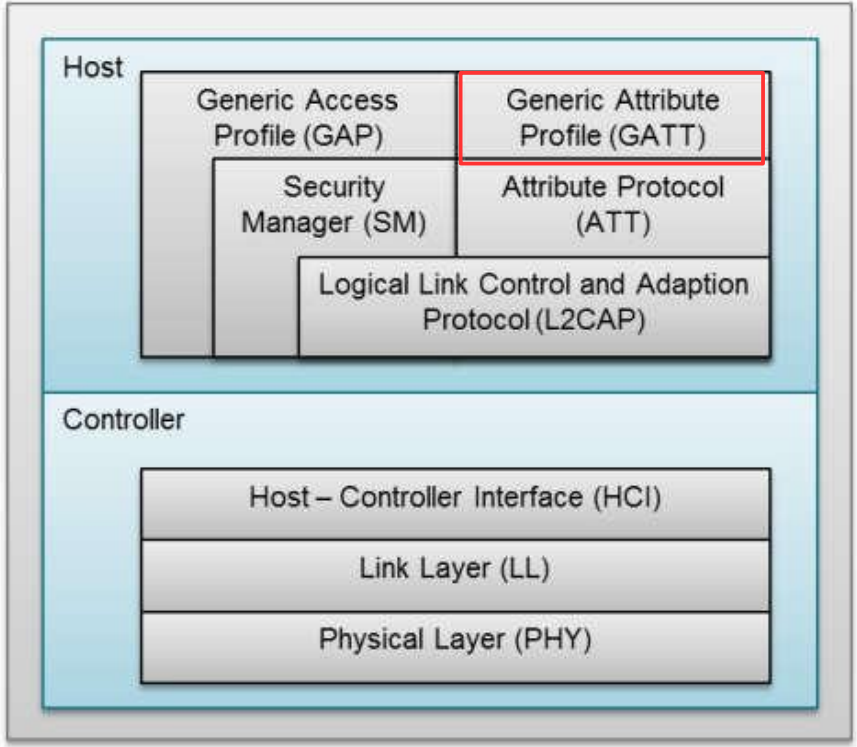
Peripheral

Central

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire *Bluetooth Low Energy*



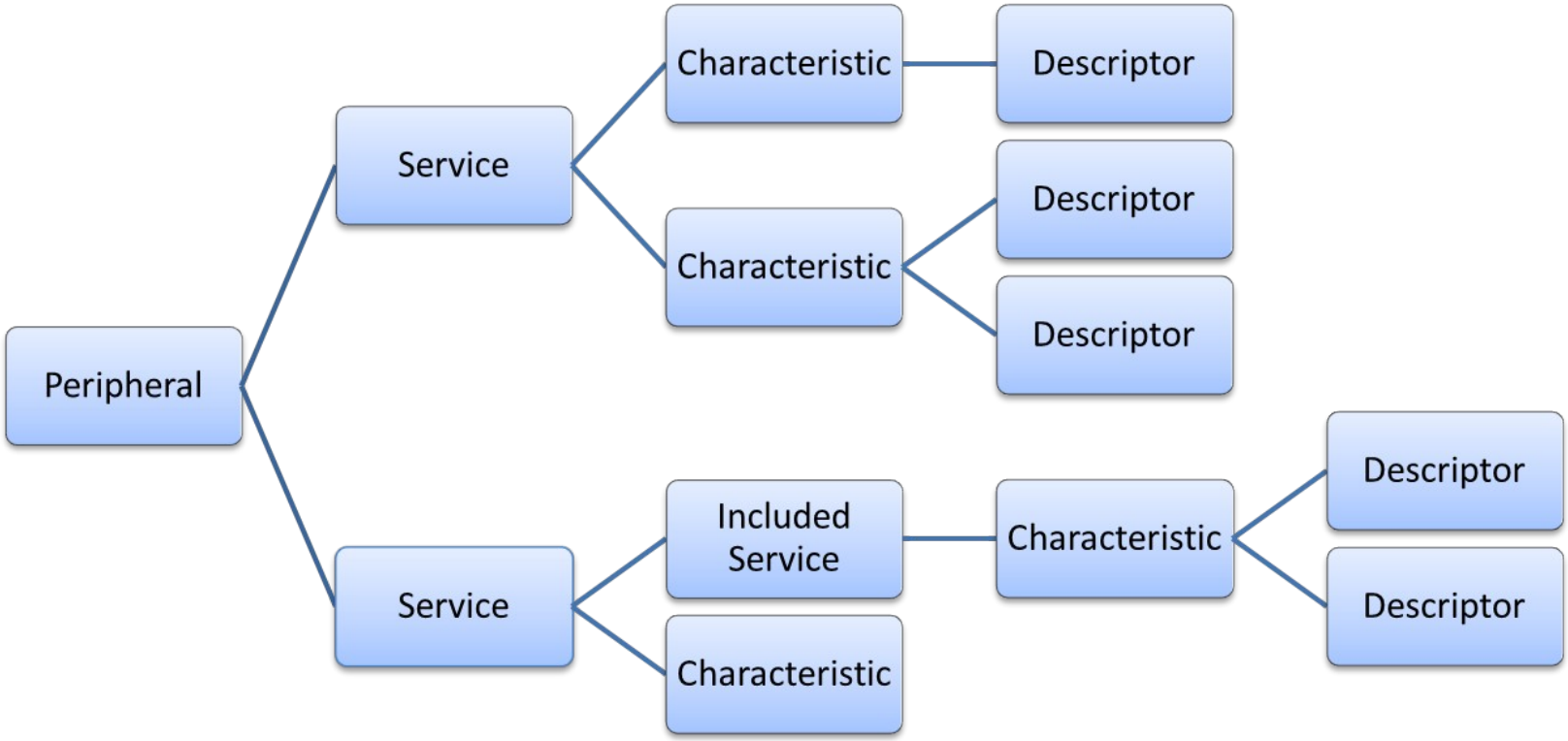
Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- *Generic ATTribute Profile* (GATT) : organisation des données

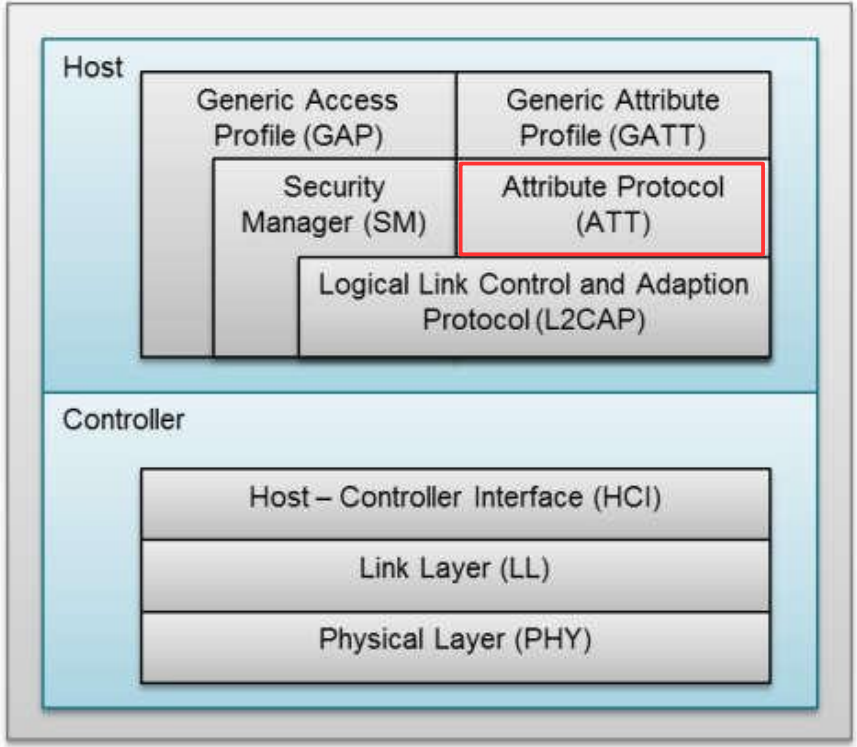


(src: Building Bluetooth LE Systems, oreilly)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire Bluetooth Low Energy



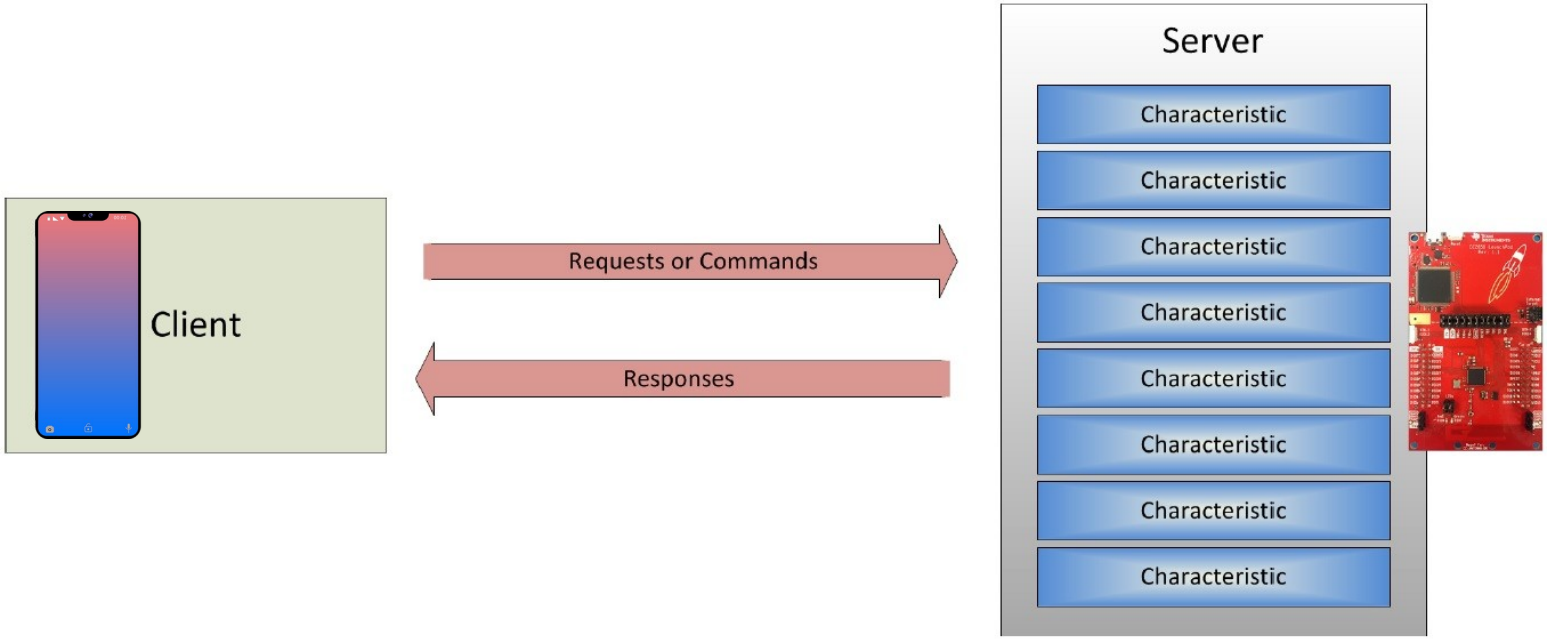
Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- *ATTribute* protocole : interaction client serveur
  - Protocole pour la découverte, la lecture et l'écriture des attributs
  - Stocke les attributs des characteristics et leur accès



(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

Generic ATTribute Profile (GATT)

GATT Heart Rate Service

		Handle	Type (UUID)	Value	Permissions
Service	Declaration	0x8000	SERVICE (0x2800)	0x180D	READ
Characteristic "Heart Rate Measurement"	Declaration	0x8001	CHAR (0x2803)	NOT|0x8002|HRM	READ
	Value	0x8002	HRM (0x2A37)	bpm	NONE
	Descriptor	0x8003	CCCD (0x2902)	0x0001	READ/WRITE
Characteristic "Body Sensor Location"	Declaration	0x8004	CHAR (0x2803)	RD|0x8005|BSL	READ
	Value	0x8005	BSL (0x2A38)	0x02 (Wrist)	READ
Characteristic "Heart Rate Control Point"	Declaration	0x8006	CHAR (0x2803)	WR|0x8007|HRC	READ
	Value	0x8007	HRC (0x2A39)	0xXX	WRITE

- Exemple :

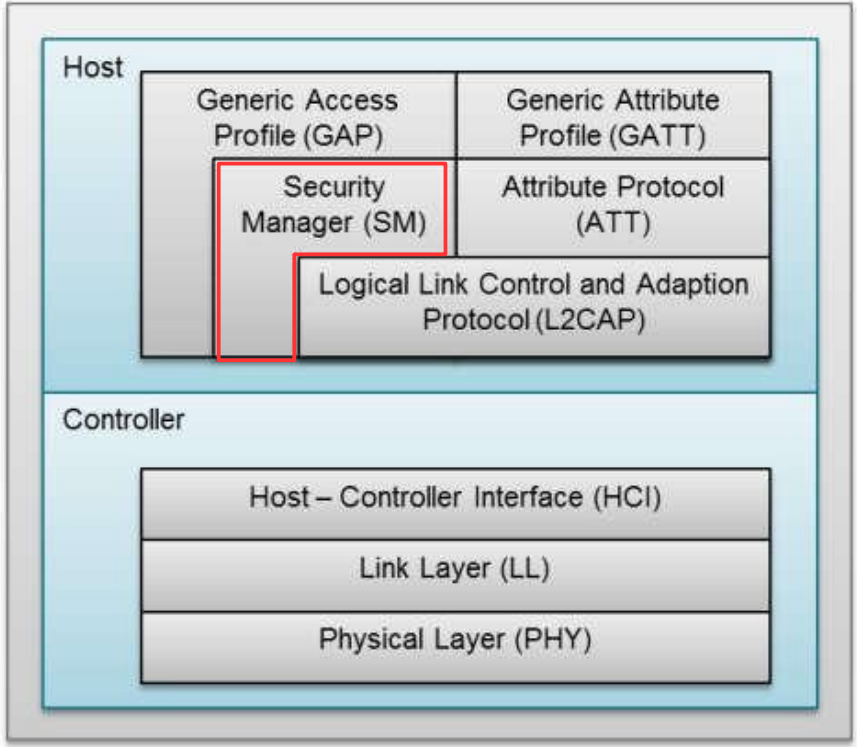
  Profil rythme cardiaque

(src: microchip)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- Pile protocolaire Bluetooth Low Energy



Bluetooth low energy protocol stack

(src: texas instrument)

© CRESITT Industrie 2024

Bluetooth BLE - Protocole

- *Security Manager Protocol* (SMP) (vol 3, part H, 2.2)
  - Utiliser pour l'appairage, la génération, le stockage et la distribution des clefs spécifiques au transport (clef de chiffrement, clef d'identité)
  - Fournit une boite à outils de
    - Fonctions de chiffrement
    - Fonctions de sécurité (*AES-CMAC RFC4493*)
    - Génération de nombres aléatoires (*hash*)
    - Génération de clefs (*Elliptic Curve Diffie Hellman (ECDH) 32bits*)
  - 2 appairages possibles :
    - *LE legacy pairing*
    - *LE Secure connection pairing*

© CRESITT Industrie 2024

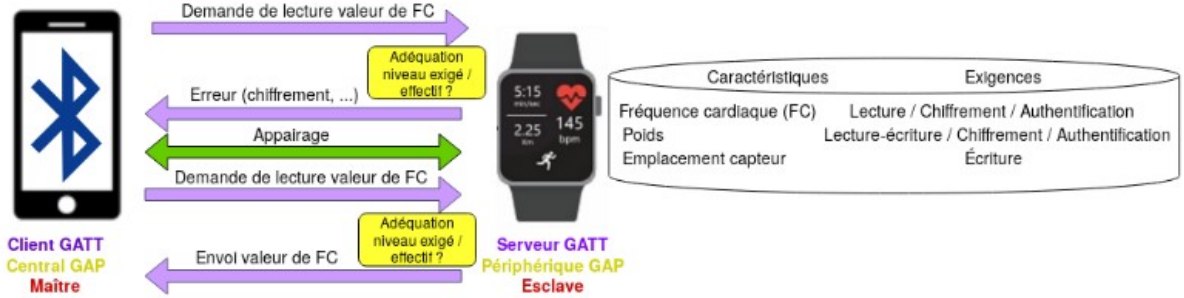
Bluetooth BLE

- La sécurité
  - Appairage : création d'une ou plusieurs clefs secrètes partagées pour chiffrer un lien.
  - Bonding : stockage des clefs pour la confiance des échanges ultérieurs
  - Authentification : vérification que les 2 parties ont les mêmes clefs
  - Chiffrement : rendre confidentiel les messages
  - Intégrité des données : protéger la falsification des données

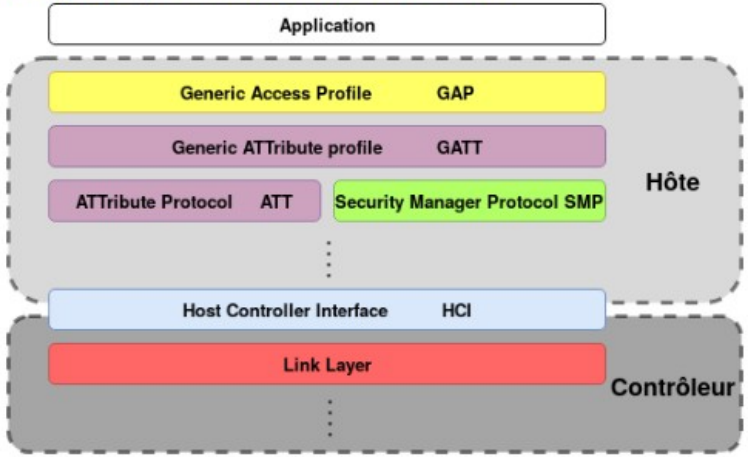
© CRESITT Industrie 2024

Bluetooth BLE - Protocole

L'imbrication des couches



La pile protocolaire du BLE



(src: ministère des armées, Nicolas DOCQ, Tristan Claverie, José LOPES-ESTEVES, Analyse des propriétés de sécurité dans les implémentations du Bluetooth Low Energy, 2 juin 2021)

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage sécurisé en 3 phases

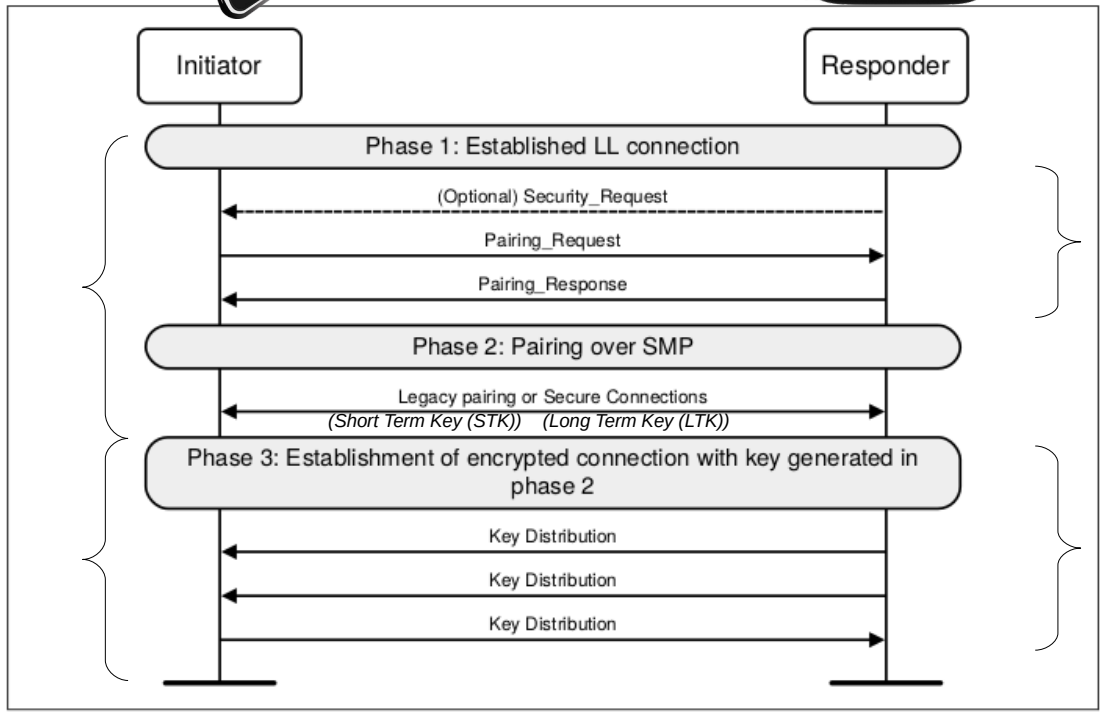


Figure 2.1: LE pairing phases

Lien chiffré ou non

Lien chiffré

Échange des exigences d'authentification et des I/O existantes qui détermine la méthode de la phase 2

Optionnel suivant la phase 2
Clefs pour chiffrer le transport et distribuer la LTK

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Modes et niveaux de sécurité applicables à chaque demande de service (GAP)

LE Security Mode	Level	Implementation
1 (Encryption)	1	No security (No authentication and no encryption)
	2	Unauthenticated pairing with encryption
	3	Authenticated pairing with encryption
	4	Authenticated LE Secure Connections pairing with encryption using a 128-bit strength encryption key
2 (Data signed)	1	Unauthenticated pairing with data signed
	2	Authenticated pairing with data signed
3 (Broadcast)	1	No security (No authentication and no encryption)
	2	Use of unauthenticated Broadcast_Code
	3	Use of authenticated Broadcast_Code
LE Secure Connection Only mode (LE security mode 1 level 4)		

Sans protection MITM (Legacy pairing – just work)

Avec protection MITM (clef STK avec authentification ou LTK avec LE Secure Connections)

Sans chiffrement

Code utilisé pour chiffrer les données

- Entraîne différents appairages

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- *Unauthentification* :
  - Mode appairage *Just Works* (accepte connexion)
  - Pas de protection contre les attaques MITM

LE Security Mode	Level	Implementation
1 (Encryption)	1	No security (No authentication and no encryption)
	2	Unauthenticated pairing with encryption
	3	Authenticated pairing with encryption
	4	Authenticated LE Secure Connections pairing with encryption using a 128-bit strength encryption key
2 (Data signed)	1	Unauthenticated pairing with data signed
	2	Authenticated pairing with data signed
3 (Broadcast)	1	No security (No authentication and no encryption)
	2	Use of unauthenticated Broadcast_Code
	3	Use of authenticated Broadcast_Code
LE Secure Connection Only mode (LE security mode 1 level 4)		

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2

  LE Legacy

  Just works

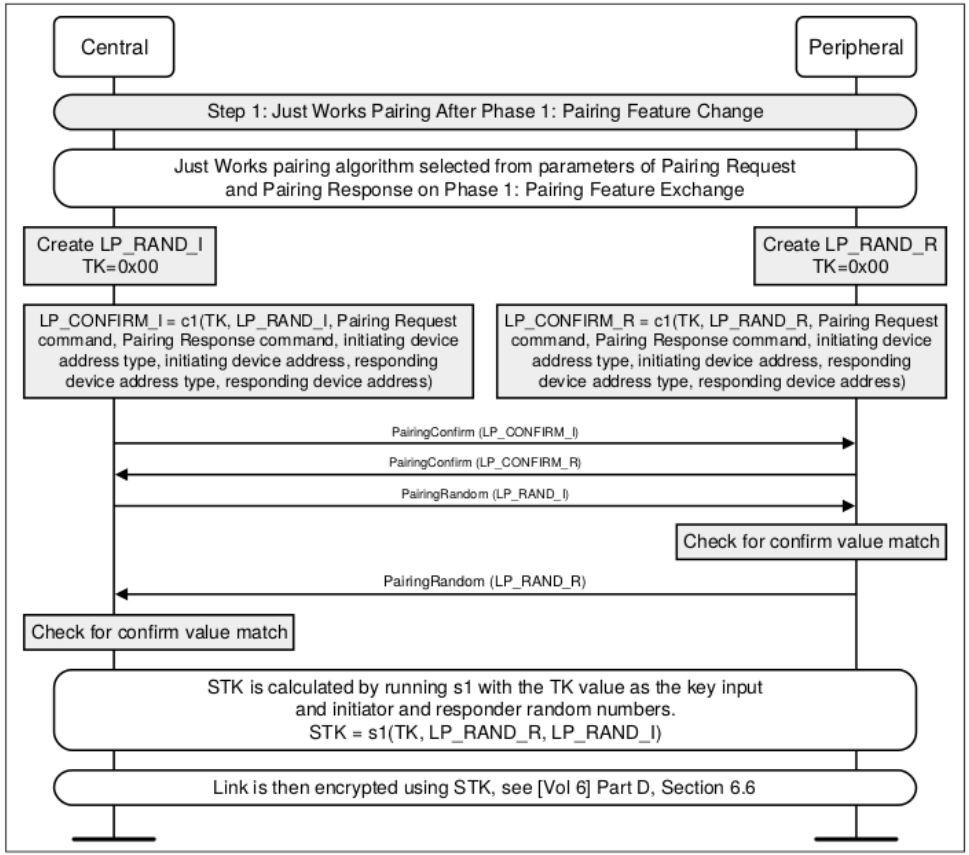


Figure C.4: Legacy Just Works pairing method

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Authentification : LE security mode 1 après connexion
  - Chiffrement :
    - Central : Session chiffrée pour échange de clef LTK qui chiffrera la connexion
    - Peripheral : Requête de sécurité esclave
      - Chiffrement de la connexion et appairage demandé par le Central ou rejet de la requête
  - Garantit intégrité et confidentialité

LE Security Mode	Level	Implementation
1 (Encryption)	1	No security (No authentication and no encryption)
	2	Unauthenticated pairing with encryption
	3	Authenticated pairing with encryption
	4	Authenticated LE Secure Connections pairing with encryption using a 128-bit strength encryption key
2 (Data signed)	1	Unauthenticated pairing with data signed
	2	Authenticated pairing with data signed
3 (Broadcast)	1	No security (No authentication and no encryption)
	2	Use of unauthenticated Broadcast_Code
	3	Use of authenticated Broadcast_Code
LE Secure Connection Only mode (LE security mode 1 level 4)		

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Requête de sécurisation émise par le *Peripheral*

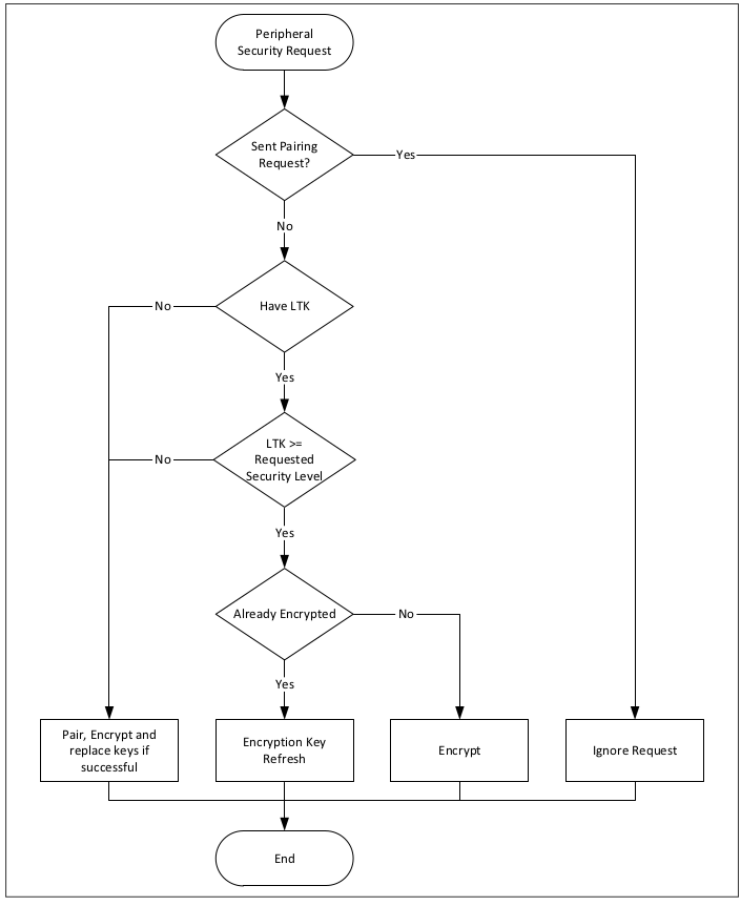


Figure 2.7: Central actions after receiving Security Request command

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- *Signed data* :
  - Utilisation d'une clef CSRK (*Connection Signature Resolving Key*)
  - Déjà présente ou générée aléatoirement
  - 128 bits
  - MAC= AES-CMAC(CSRK,(pdu||SignCounter),64bits)

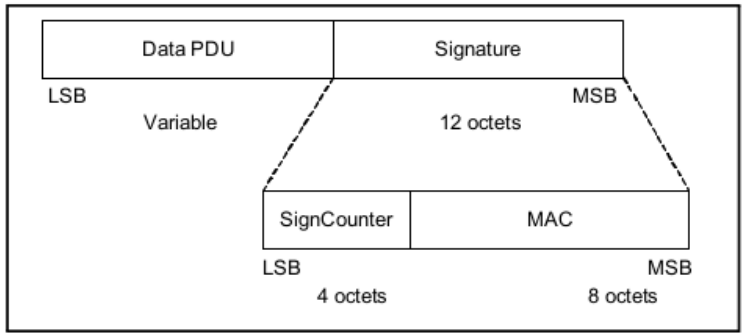


Figure 10.3: Generic format of signed data

LE Security Mode	Level	Implementation
1 (Encryption)	1	No security (No authentication and no encryption)
	2	Unauthenticated pairing with encryption
	3	Authenticated pairing with encryption
	4	Authenticated LE Secure Connections pairing with encryption using a 128-bit strength encryption key
2 (Data signed)	1	Unauthenticated pairing with data signed
	2	Authenticated pairing with data signed
3 (Broadcast)	1	No security (No authentication and no encryption)
	2	Use of unauthenticated Broadcast_Code
	3	Use of authenticated Broadcast_Code
LE Secure Connection Only mode (LE security mode 1 level 4)		

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage Phase 1 : échange des paramètres

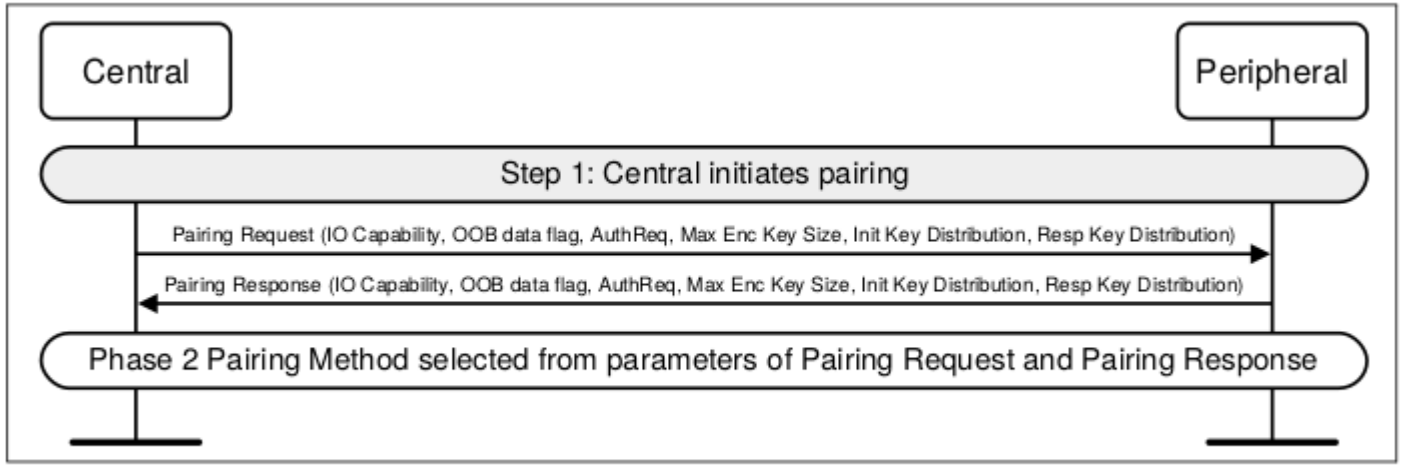


Figure C.2: Pairing initiated by Central

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- 2 possibilités d'appairage
  - *LE Legacy pairing* : simple appairage : 3 modèles d'associations
    - *Just Works* : simple acceptation de connexion (aucune IHM disponible), TK=0, tout le monde peut se connecter
    - *Passkey Entry* : code à 6 chiffres à saisir, fourni depuis un device puis saisi sur l'autre, TK sur 6 chiffres
    - *Out-of-Band* : utilisation d'une authentification externe (ex : NFC) qui retourne « yes » or « no »
      - TK échanger par un autre moyen (ex : NFC)
      - Protection contre les attaques MITM
    - Utilise 2 clefs (Key)
      Temporary Key (TK) : 128-bits utilisés pour générer STK
      Short Term Key (STK) : 128-bits utilisés pour chiffrer une connexion après l'appairage
    - Pas de protection contre l'écoute passive

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- 2 possibilités d'appairage
  - *LE Legacy pairing* : simple appairage : 3 modèles d'associations
  - *LE Secure Connexions* : 4 modèles d'associations
    - *LE Legacy pairing + Numeric Comparison* : saisie de caractère au clavier (6 digit) sur les 2 devices
    - *Long term Key (LTK)* : clef 128 bits pour chiffrer la connexion après l'appairage et pour les futures connexions

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Legacy
  Passkey Entry

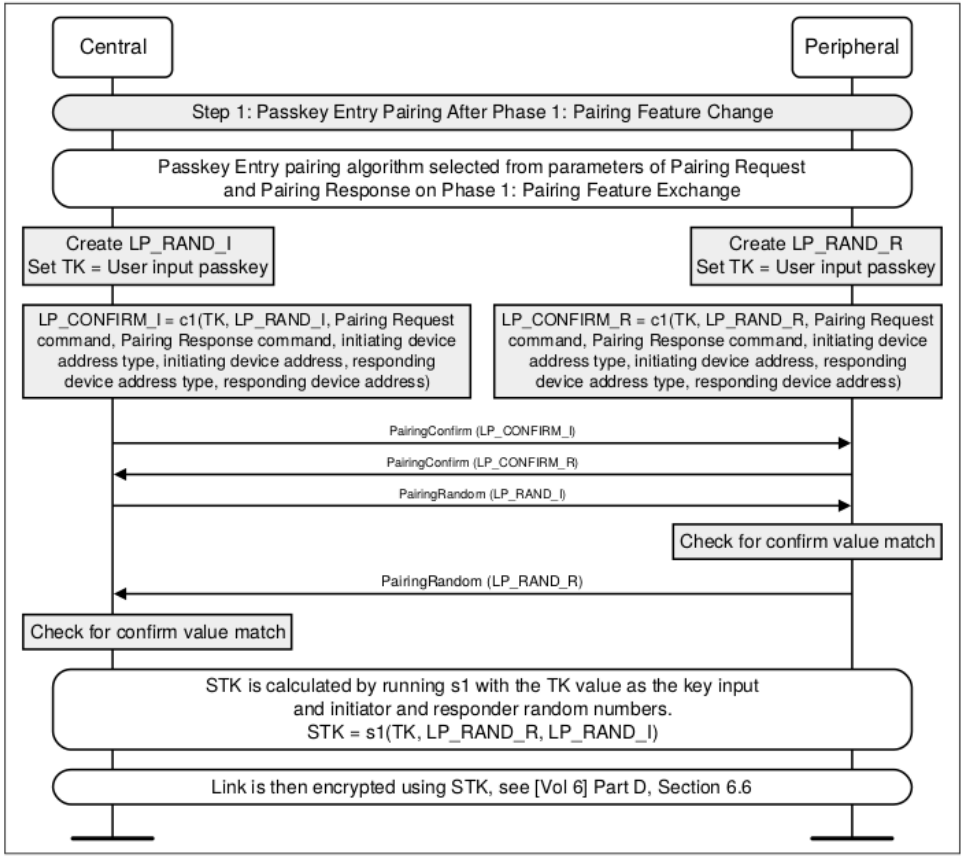


Figure C.5: Legacy Passkey Entry pairing method

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Legacy
  Out of Band

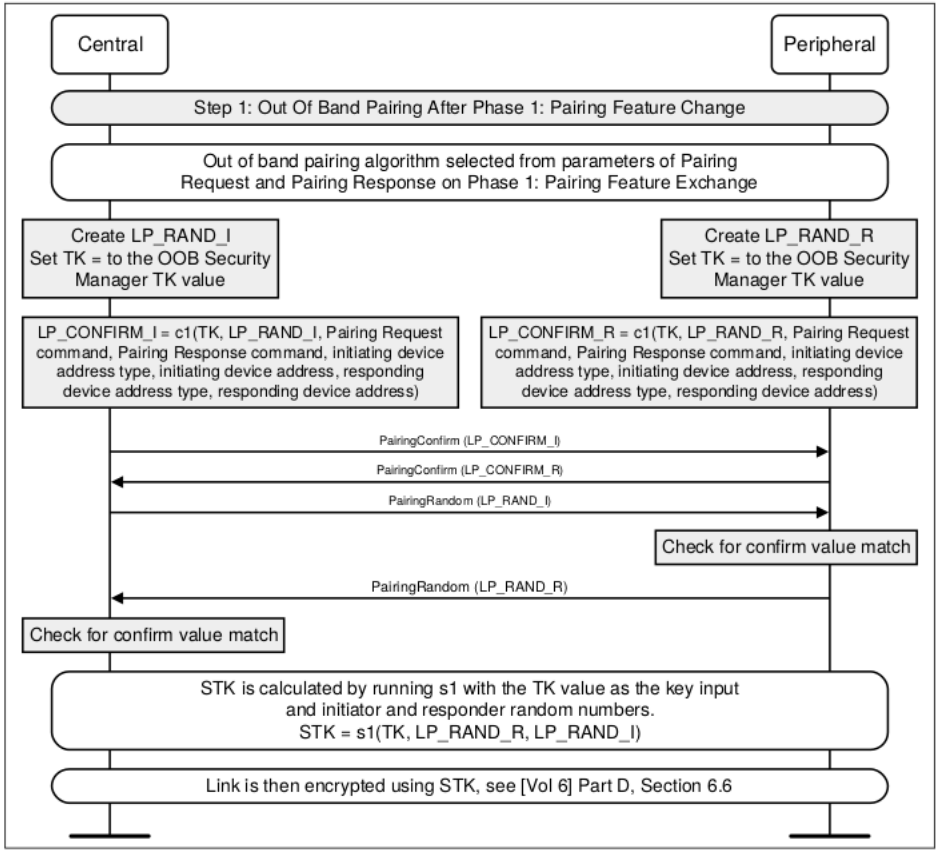


Figure C.6: Legacy OOB pairing method

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Secure Connections
  Just work ou *Numeric comparison*

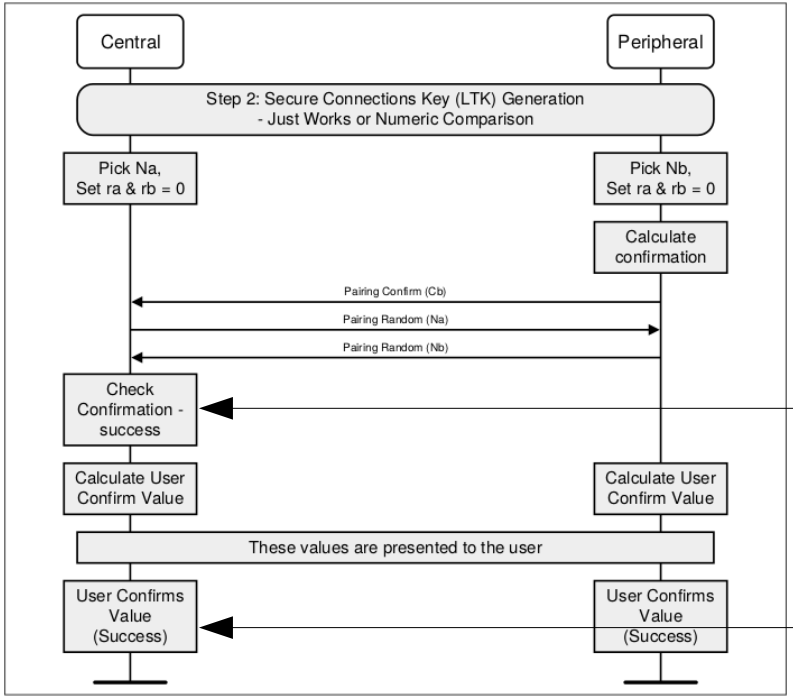


Figure C.8: Pairing Phase 2, authentication stage 1, successful Numeric Comparison

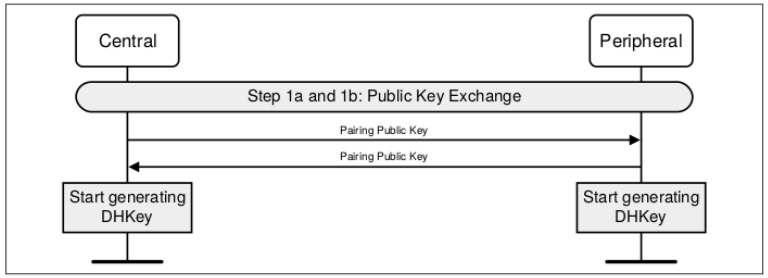


Figure C.7: Pairing Phase 2 – Public Key Exchange

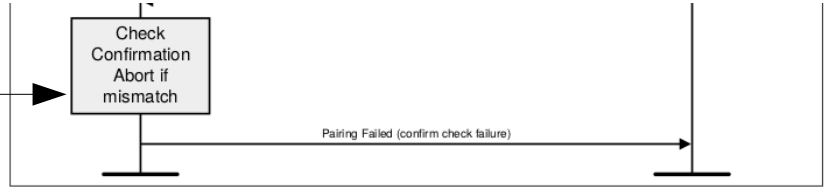


Figure C.9: Pairing Phase 2, authentication stage 1, Numeric Comparison – Confirm Check failure on Initiator side

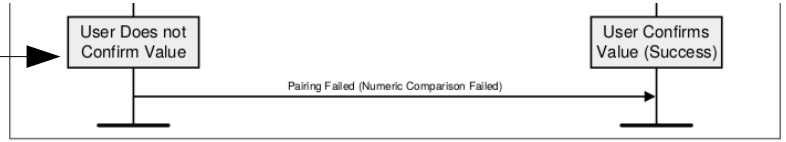


Figure C.10: Pairing Phase 2, authentication stage 1, Numeric Comparison failure on Initiator side

Inverse si *peripheral* ne confirme pas

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Secure Connections
  Passkey Entry

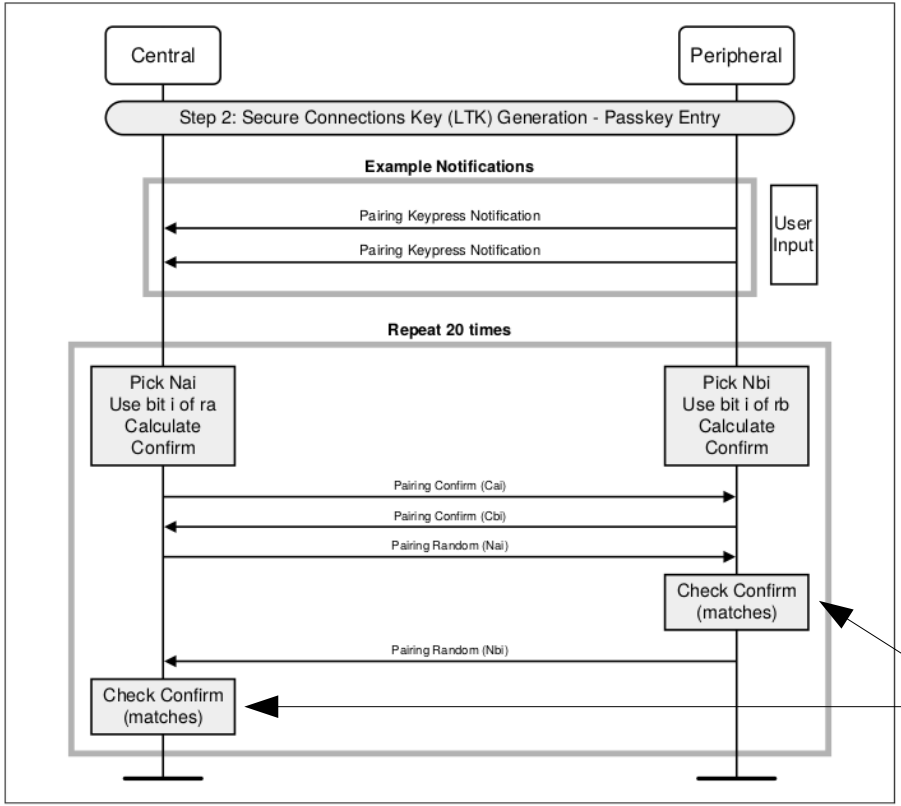


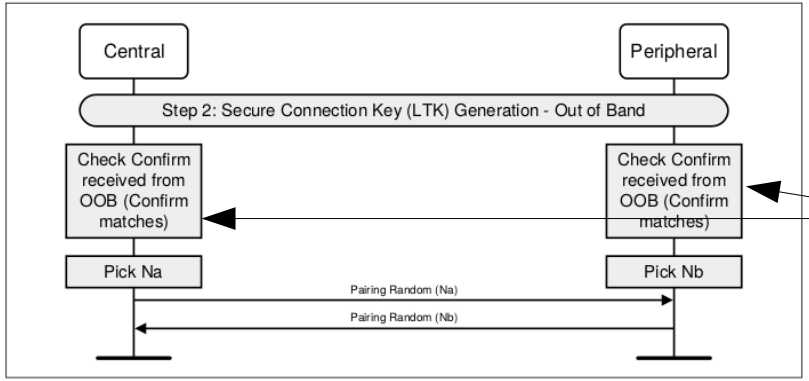
Figure C.12: Pairing Phase 2, authentication stage 1, Successful Passkey Entry

Peut ne pas matcher et renvoyer *Pairing failed*

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Secure Connections
  OOB



Peut ne pas matcher et renvoyer *Pairing failed*

Figure C.17: Pairing Phase 2, authentication stage 1, successful Out of Band

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Secure Connections

  stage 2

  calcul d'une clef Diffie Hellman pour le calcul de la LTK

Numeric Comparison	Out-Of-Band	Passkey Entry
Ea = *f3*(DHKey, Na, Nb, 0, IOcapA, A, B)	Ea = *f3*(DHKey, Na, Nb, rb, IOcapA, A, B)	Ea = *f3*(DHKey, Na20, Nb20, rb, IOcapA, A, B)
Eb = *f3*(DHKey, Nb, Na, 0, IOcapB, B, A)	Eb = *f3*(DHKey, Nb, Na, ra, IOcapB, B, A)	Eb = *f3*(DHKey, Nb20, Na20, ra, IOcapB, B, A)

Table 7.7: Inputs to f3 for the different protocols

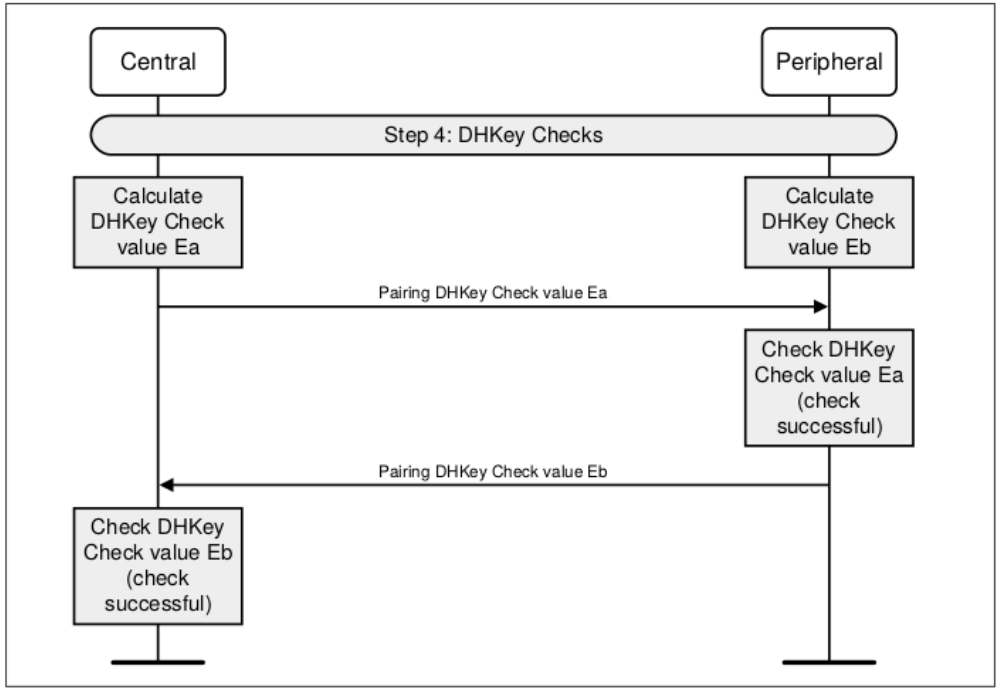


Figure C.23: Pairing Phase 2, authentication stage 2, DHKey checks

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 2
  LE Secure Connections

  stage 2

  Obtention de la clef LTK

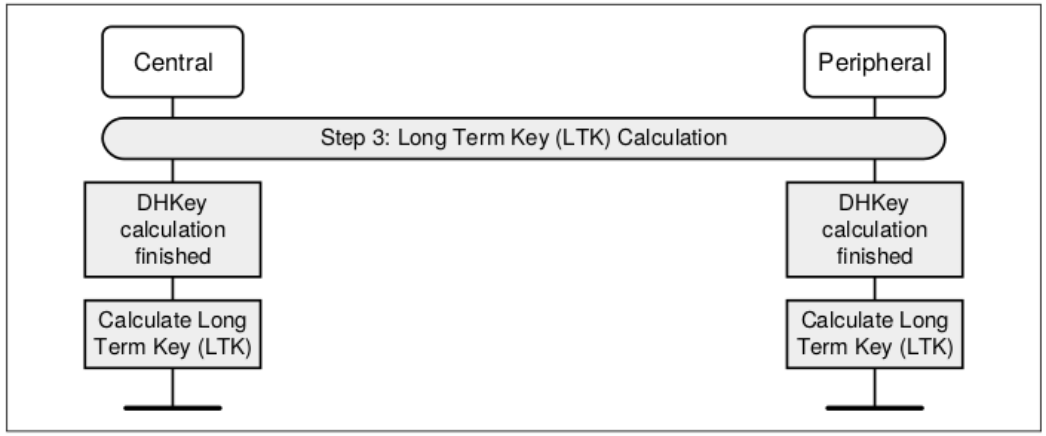


Figure C.22: Long Term Key calculation

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Terminologie des fonctions

Term	Definition
DHKey	Diffie Hellman key
Ex	Check value from device X
f1( )	Used to generate the 128-bit commitment values Ca and Cb
f2( )	Used to compute the link key and possible other keys from the DHKey and random nonces
f3( )	Used to compute check values Ea and Eb in Authentication stage 2
g( )	Used to compute numeric check values
IOcapA	IO capabilities of device A
IOcapB	IO capabilities of device B
LK	Link Key
Nx	Nonce (unique random value) from device X
Nxi	i^{th} nonce (unique random value) from device X. Only used in the passkey entry protocol
PKx	Public Key of device X
rx	Random value generated by device X
rxi	Bit i of the random value rx. Only used in the passkey entry protocol
SKx	Secret (Private) Key of device X
Vx	Confirmation value on device X. Only used in the numeric compare protocol.
X	BD_ADDR of device X

Table 7.1: Terminology

© CRESITT Industrie 2024

Long Term Key (LTK) 128 bits

- Une fois la communication chiffrée avec STK on va pouvoir échanger la LTK qui est une valeur aléatoire stockée dans un base de sécurité.

- Les IotT ayant peu de ressources (les esclaves) fournissent aux maîtres deux autres valeurs EDIV (16bits) et RAND (64 bits) que le maître renverra à la prochaine connexion et qui permet à l'esclave de recalculer sa LTK. Nouvelle EDIV pour chaque distribution de nouvelle LTK.

- Les deux autres clés (IRK et CSRK) sont échangées et sauvegardées pendant cette phase.

- A l'issue les objets sont dits « BONDED » et utiliseront les LTK à la prochaine connexion.

© CRESITT Industrie 2024

Identity Resolving Key (IRK) 128 bits

- Pour ne pas être tracés les objets vont en général fournir une adresse privée aléatoire qui peut changer n'importe quand.
- Si un objet détient L'IRK d'un autre il sera capable de l'**identifier** car une partie de l'adresse est formée à partir de L'IRK
- Un objet peut distribuer des IRK différents à chaque partenaire.

© CRESITT Industrie 2024

Connection Signature Reloving Key (CSRK) 128 bits

- La CSRK permet de signer le message envoyé et donc d'**authentifier** son émetteur.
- Ce mécanisme est intéressant en cas déconnexion/ reconnexion
- Le message authentifié peut être envoyé en clair.

© CRESITT Industrie 2024

Bluetooth BLE

- Hiérarchie de clefs

Mrand Srand : nombres aléatoires (64 bits)

N1-N2 : 128 bits (*nonce*)

SALT : 128-bit value:
0x6C888391_AAF5A538_60370BDB_5A6083BE

STK : courte durée de vie
non vulnérable à
l'attaque MITM

EDIV : encrypted diversifier sur 16bits

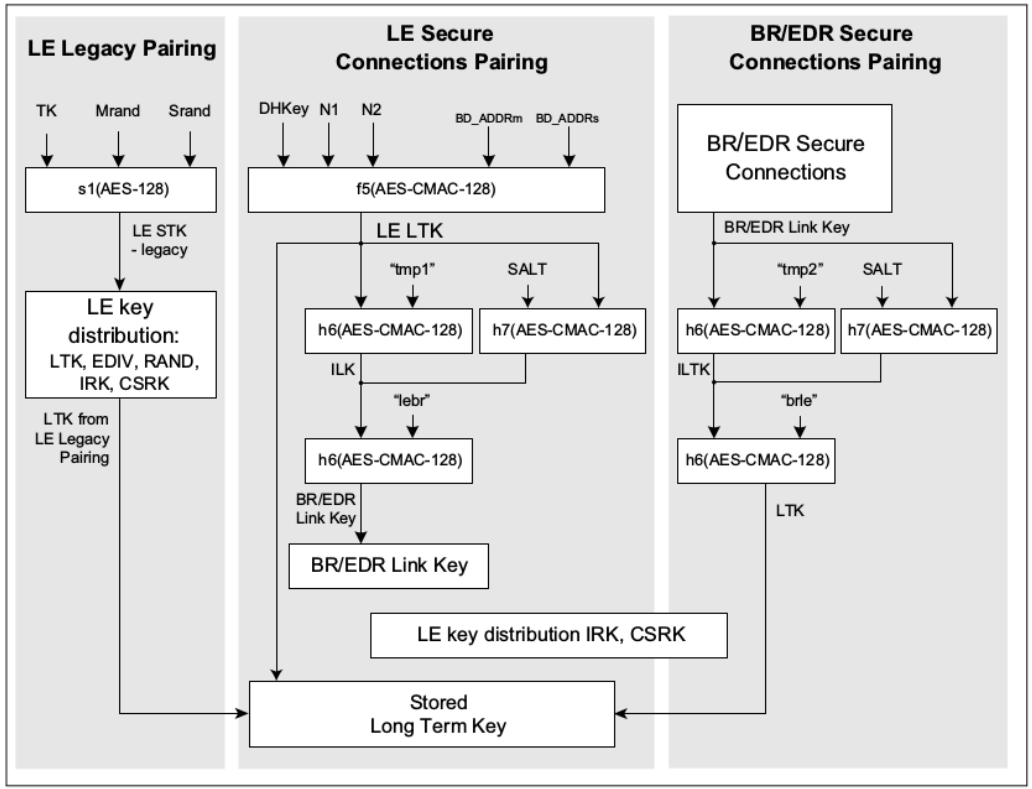


Figure 5.2: LE key hierarchy

(src: bluetooth core specification 5.1)

© CRESITT Industrie 2024

Bluetooth BLE - Sécurité

- Appairage phase 3
  Distribution des clefs spécifiques de transport après chiffrement du lien

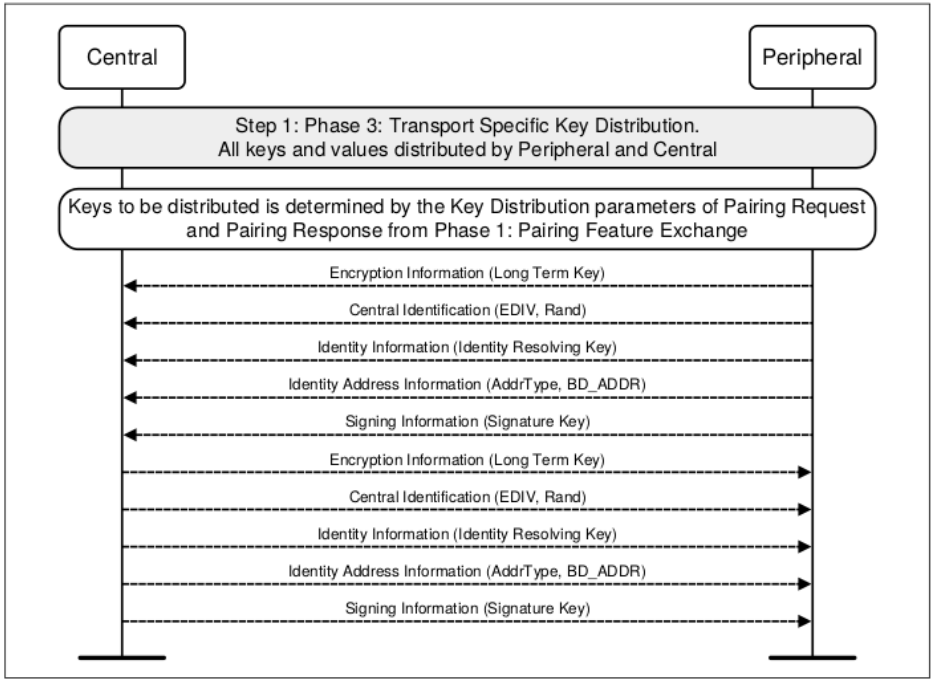


Figure C.24: Transport specific key distribution

© CRESITT Industrie 2024

Bluetooth BLE - Vulnérabilités

- CVE liste : https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/

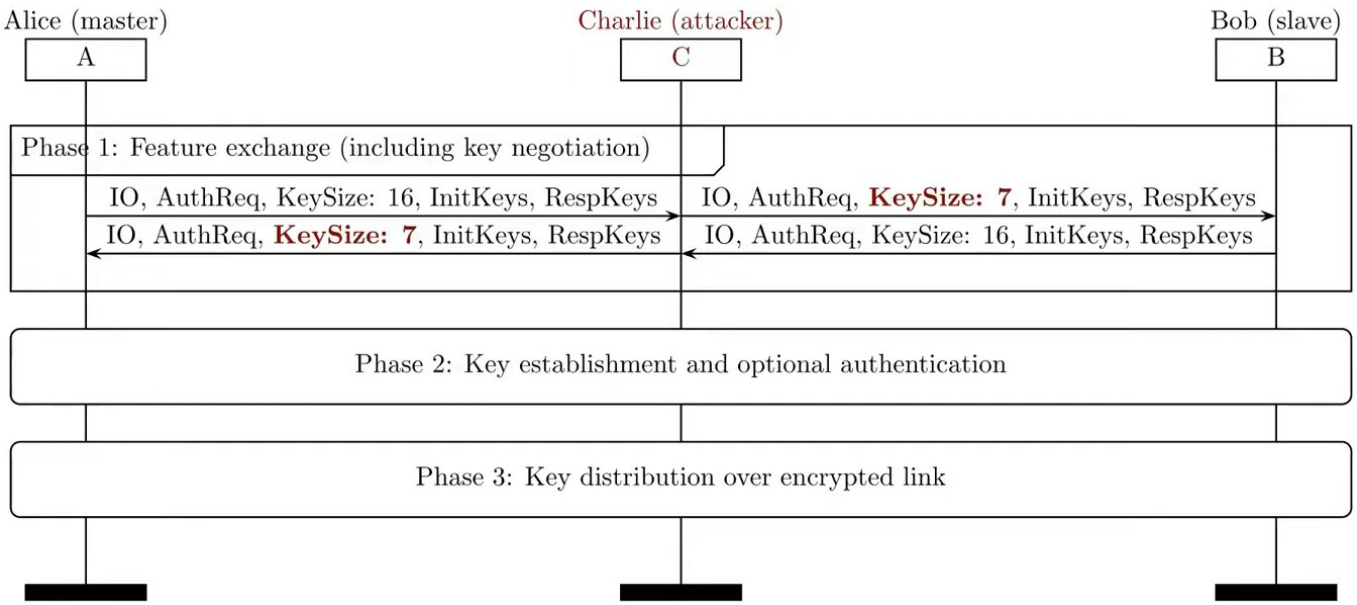
Bluetooth Security Notices

Vulnerability	Publication Date	Details	Specifications Affected	CVE [NVD]
SUPPLEMENT: Impersonation in the Passkey Entry Protocol	19/09/2024	SIG Security Notice	Core Spec v2.1 to 5.4	CVE-2021-37577
BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses	27/11/2023	SIG Security Notice	Core Spec v4.2 to 5.2	CVE-2023-24023
Pairing Mode Confusion in BLE Passkey Entry	09/12/2022	SIG Security Notice	Core Spec v4.0 to 5.3	CVE-2022-25836
Pairing Mode Confusion in BR/EDR	09/12/2022	SIG Security Notice	Core Spec v1.0B to 5.3	CVE-2022-25837
InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections	21/06/2021	SIG Security Notice	Core Spec, v4.0 to 5.2	CVE-2021-31615

© CRESITT Industrie 2024

Bluetooth BLE - Vulnérabilités

- *Key Negociation Of Bluetooth (**KNOB**) attack* CVE 2019-9506



- Diminue taille de la clef au minimum (non chiffrée)
- Facilite attaque brute force de la clef de session

(src: Daniele Antonioli)

© CRESITT Industrie 2024

Bluetooth BLE - Vulnérabilités

- *Bluetooth Low Energy Spoofing Attack (**BLESA**)* CVE-2020-9770
  - Description vague du processus de reconnexion par la norme (<=v5.2)
  - Possibilité de ne pas se ré-authentifier à la reconnexion
  - La ré-authentification, si elle est demandée, peut être ignorée
  - Possibilité de se faire passer pour le précédent device connecté.
  - Pas forcément simple de corriger la faille sur tous les produits

© CRESITT Industrie 2024

Bluetooth BLE - Vulnérabilités

- ***BLURtooth*** CVE-2020-15802
  - Appairage de 2 devices en Bluetooth et en BLE simultanément (v4.2 ≤ x ≤ v5.0)
  - Faille de l'utilisation de la clef de dérivation inter-transport (CTKD)
  - Attaque MITM
  - Norme autorise le bonding d'un utilisateur non authentifié sur une couche de transport. L'attaquant peut alors potentiellement :
    - remplacer le bonding sur l'autre couche transport,
    - écraser la clef d'authentification par une clef non-authentifiée
    - diminuer l'entropie

© CRESITT Industrie 2024

Bluetooth BLE - Sniffer

- Teledyne Lecroy
  Analyseur de protocole sans fil **Frontline X240**

Summary

All Frames | Technology: LE | Search

LE: LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT | Errors | 5 frames displayed

B...	Frame#	Side	Code	Fram...	Delta	Timestamp
	976	1	Pairing Request	52		09/05/2022 13:01:40.550298
	996	2	Pairing Response	52	00:00:00.226362	09/05/2022 13:01:40.776660
	1,000	* 1	* Pairing Public Key	56	00:00:00.090504	09/05/2022 13:01:40.867164
	1,016	1	Pairing Random	62	00:00:00.313133	09/05/2022 13:01:41.180297
	1,054	1	Pairing DHKey Check	62	00:00:01.889992	09/05/2022 13:01:43.070289

Decode

- Frame 976: Len=52
- LE BB:
- LE PKT:
- LE DATA:
- L2CAP:
- SMP:
  - Code: Pairing Request
  - IO Capabilities: KeyboardDisplay
  - OOB data flag: OOB Authentication data not present
  - AuthReq
    - Bonding_Flags: Bonding
    - MITM: MITM Protection: Yes
    - Secure Connection Pairing: Yes
    - Keypress Notifications: No
    - CT2: Supports h7 Function: Yes
  - Maximum Encryption Key Size: 16 Octets
  - Initiator Key Distribution
    - EncKey: Initiator shall distribute LTK followed by EDIV and Rand
    - IdKey: Initiator shall distribute IRK followed by its address
    - Sign: Initiator shall distribute CSRK
    - LinkKey: Initiator would like to derive key from LTK
  - Responder Key Distribution
    - EncKey: Responder shall distribute LTK followed by EDIV and Rand
    - IdKey: Responder shall distribute IRK followed by its address
    - Sign: Responder shall distribute CSRK
    - LinkKey: Responder would like to derive key from LTK

© CRESITT Industrie 2024

CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique

CRT centre de ressources technologiques

Journée sur la sécurité des piles réseaux
(Journée commune au GDR RSD, GPL (GT GLSEC) et SI (GT SSLR))

La sécurité dans le Bluetooth Low Energy
FIN

Le CRT CRESITT est soutenu par :

Ministère de l'Enseignement supérieur et de la Recherche — Cofinancé par l'Union européenne — Région Centre Val de Loire — Orléans Métropole

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

© CRESITT Industrie – FE01 11 IndH