Segurança em redes sem fios - Bluetooth

Jaime Dias

FEUP > DEEC > MRSC > **Segurança em Sistemas e Redes**

v3

Segurança em redes sem fios

- Comunicações sem fios
  - vantagens:
    - *Comodidade*
    - *Mobilidade*
  - desvantagens:
    - *facilidade em observar ou alterar dados alheios*
    - *facilidade em interferir no meio*
    - *acesso por utilizadores estranhos*

Bluetooth

Enquadramento

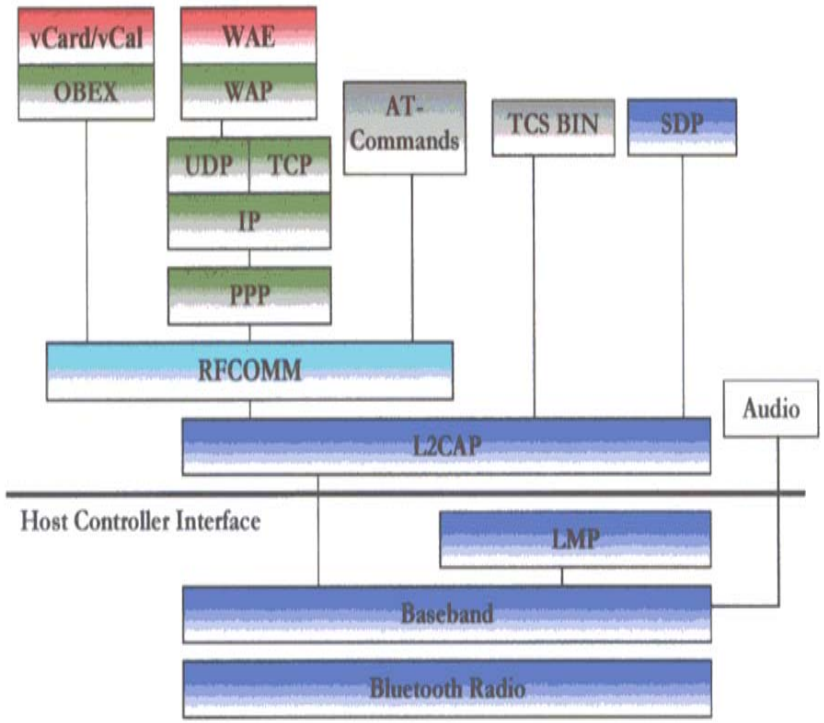
- IEEE 802.15
- *WPAN (Wireless Personal Area Network)*
- Complemento ao 802.11 (WLAN) e não uma alternativa
- Faixa dos 2,4 GHz (ISM - *Industrial-Scientific-Medical*)
- Débito: 1 Msample/s → 720 kbit/s (v2.0 → 2,1 Mbit/s)
- Tecnologia para substituição do cabo → pequenas redes locais (pessoais) → piconet

Enquadramento

- 3 classes
  - Classe 1: 100 mW ➔ 100 m
  - Classe 2: 2.5 mW ➔ 10 m
  - Classe 3: 1 mW ➔ 0,1 – 10 m
- Arquitectura Mestre/Escravo
- Actualmente: quant. dispositivos BT > estações 802.11
  - Telefones, *headsets*, portáteis, ratos, teclados, etc.

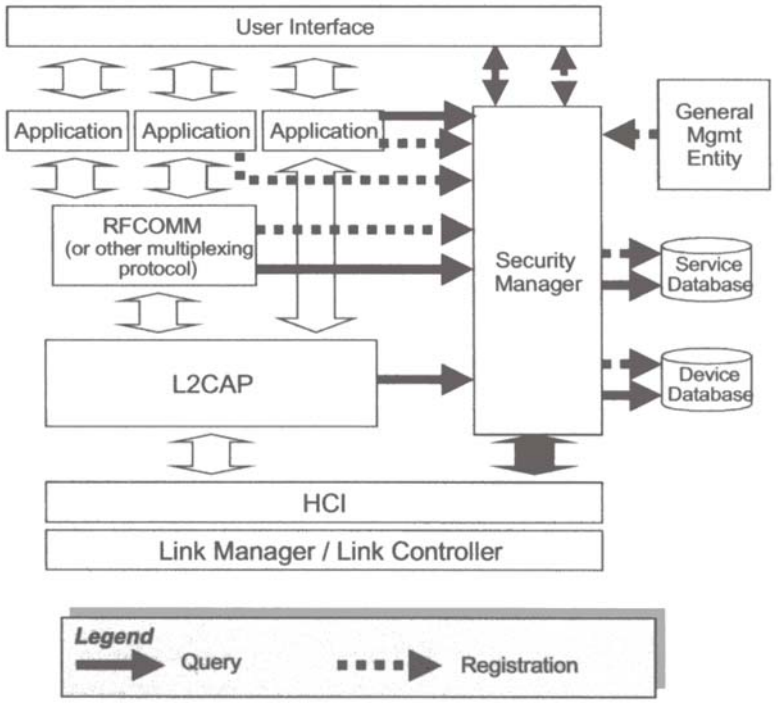
Pilha protocolar

- **Baseband** ➔ permite o estabelecimento de ligações físicas (RF) entre dispositivos.
- **LMP** (*Link Manager Protocol*) ➔ responsável pelo estabelecimento de ligações. Entre outras funcionalidades estão as da segurança.
- **Host Controller Interface (HCI)** ➔ API para acesso ao controlador Baseband, *Link Manager* e outros controladores de *hardware*.
- **L2CAP** (*Logical Link Control and Adaptation Protocol*) ➔ Adapta protocolos (encapsula) da camada superior ao Baseband.
- **SDP** (*Service Discovery Protocol*) ➔ protocolo para a descoberta de dispositivos buetooth na rede: tipo de dispositivo, serviços e respectivos parâmetros de forma a permitir o estabelecimento de ligações
- **RFCOMM** ➔ protocolo para substituição do cabo. Emulação do RS232
- **TCS BINARY e comandos AT** ➔ para utilização de modems sobre bluetooth



Arquitectura de segurança

- *Security Manager* → responsável pela gestão da segurança de um dispositivo bluetooth
- Autenticação ao nível do dispositivo e não do utilizador
- Identificação de cada dispositivo: endereço MAC (único) (48 bits)
  → BD_ADDR



Modos de segurança

- 3 modos de segurança
  - Modo1 - Sem segurança
  - Modo 2 - Segurança ao nível do serviço
    - *Após o estabelecimento da ligação lógica (LMP) e de um canal L2CAP*
    - *Políticas de segurança ao nível da aplicação.*
  - Modo 3 - Segurança ao nível da ligação
    - *Antes do estabelecimento de uma ligação lógica (LMP)*

Modos de segurança (2)

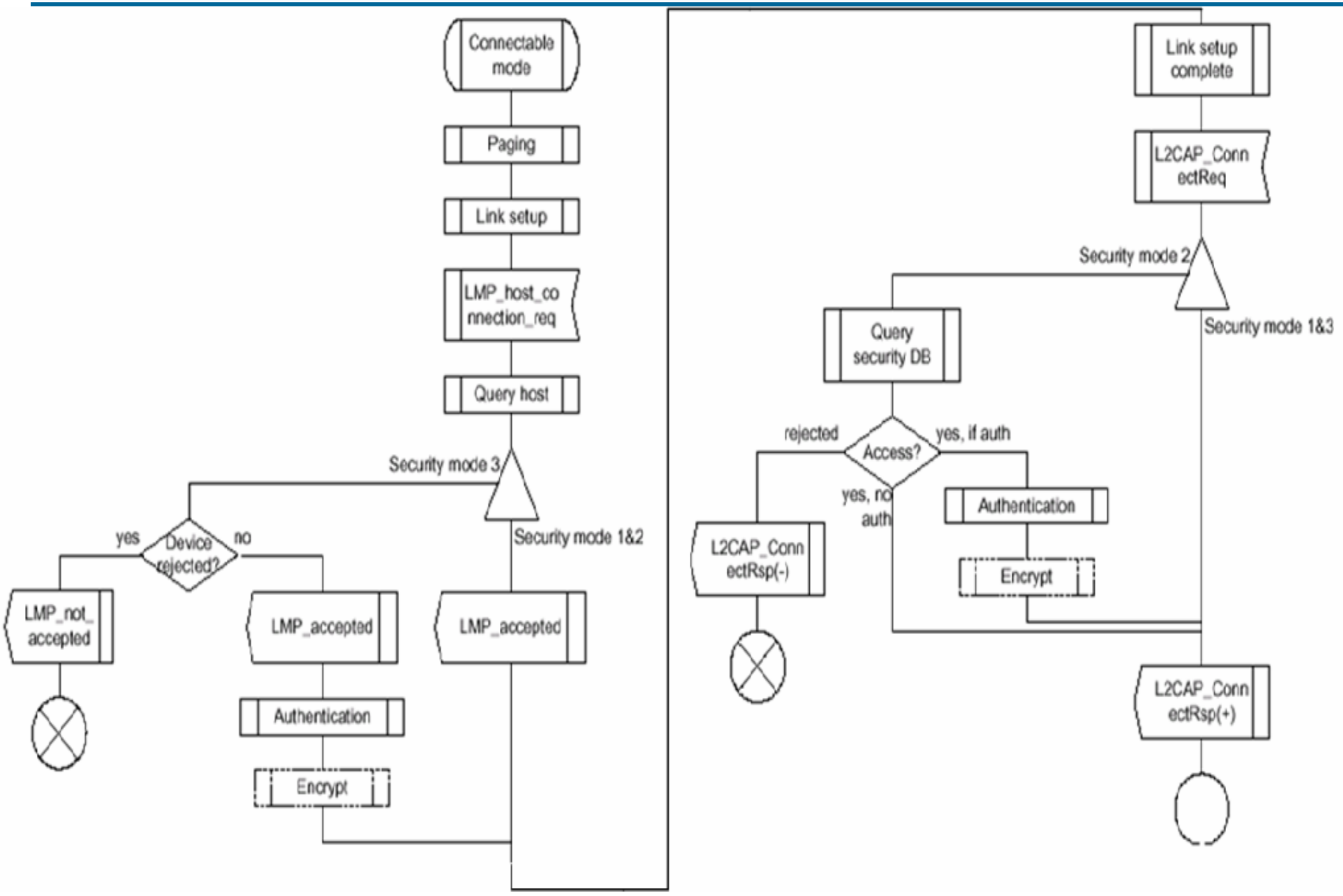
Confiança

- Ao nível do dispositivo
- *Trusted*: acesso a todos os serviços. Dispositivo autenticado e marcado como "*trusted*".
- *Untrusted*: acesso limitado aos serviços. Autenticado mas marcado como "*untrusted*".
- Unknown: acesso limitado aos serviços. Dispositivo desconhecido (não autenticado). Tratado como "*untrusted*"

Modos de segurança (3)

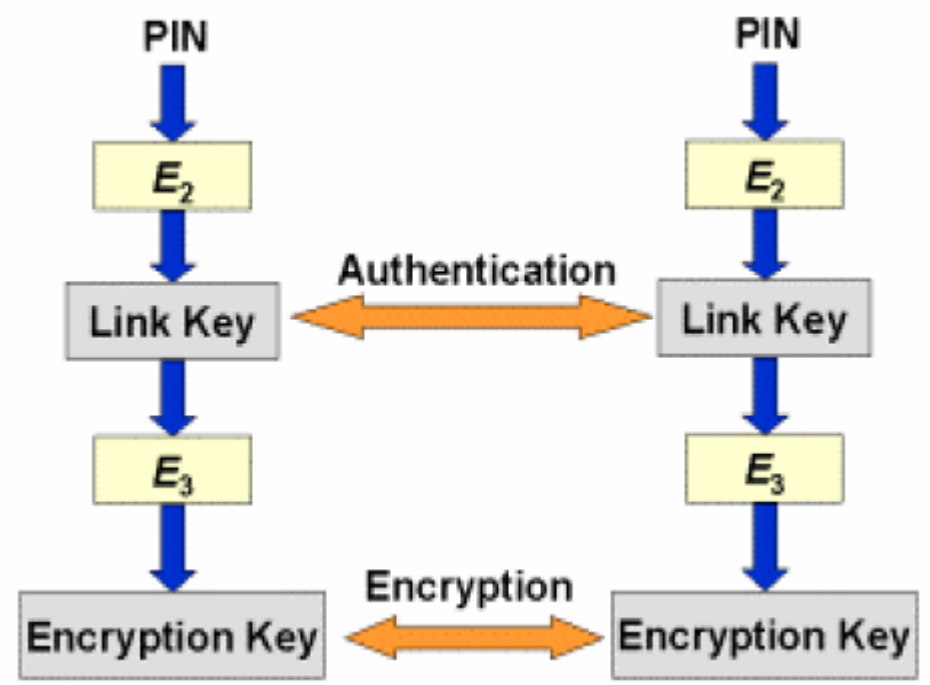
- Modo 2 → cada serviço (aplicação) define que tipo de segurança pretende. Especifica nenhum, um ou vários dos seguintes atributos:
  - autenticação
  - autorização (implica autenticação)
    - *Trusted devices → autorização automática*
    - *Untrusted ou Unknown devices → autorização manual*
  - cifragem (confidencialidade e integridade) (implica autenticação)

Modos de segurança (3)



Chaves

- Criptografia simétrica
- 3 tipos de chave
  - Código PIN
  - Ligação (*Link key*)
  - Cifragem (*Encryption key*)



Código PIN

- O segredo partilhado entre dispositivos confiáveis (*trusted*)
- Fixado por dispositivo ou selecionado pelo utilizador
- de 8 a 128 bits (1 a 16 octetos) → normalmente 4 dígitos

Chaves de ligação (*link keys*)

- Para autenticação e derivação de chaves de confidencialidade
- Números pseudoaleatórios de 128 bits
- Chave de inicialização (*Initialization key*) K_{init}
  - Utilizada no processo de inicialização. Usada apenas uma vez.
- Chave de unidade (*Unit key*) K_A
  - Única, de longo-prazo, gerada aquando da instalação dos dispositivo
- Chave combinada (*Combination key*) K_{AB}
  - Derivada para comunicação entre dois periféricos (A e B)
  - Requer mais memória que uma *Unit key*, mas é mais segura
- Chave de mestre (*Master key*) K_{master}
  - Temporária: válida apenas para uma sessão
  - Utilizada quando mestre quer comunicar com vários dispositivos

Chave de cifragem (*Encryption key*)

- Derivada da chave de ligação
- De cada vez que é necessária confidencialidade é gerada uma nova chave de cifragem
- Independente da chave de ligação (de autenticação) ➔ chave de cifragem pode ser menor (melhor desempenho) sem com isso comprometer a segurança do sistema

Procedimentos de segurança (unicast)

Primeira vez

1. Geração da chave de inicialização (K_{init}) (*pairing*)
2. Autenticação com K_{init}
3. Geração/troca de uma chave de ligação
   - Chave de unidade (K_A) ou chave combinada (K_{AB})
4. Geração de chave de cifragem
5. Cifragem dos dados

Procedimentos de segurança (unicast)

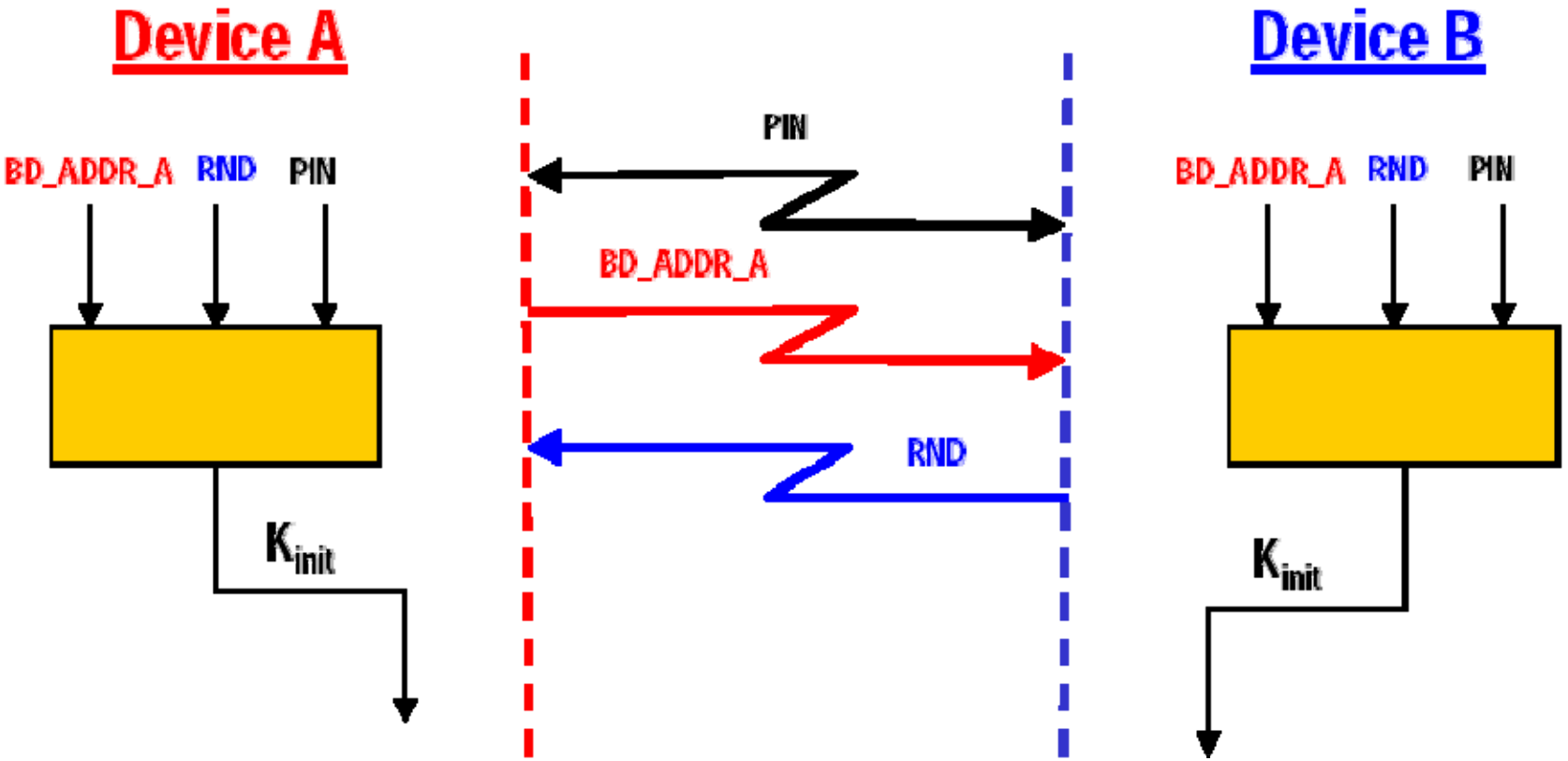
Vezes seguintes

1. Autenticação com chave de unidade (K_A) ou chave combinada (K_{AB})
   - Idêntica à autenticação com chave de inicialização
2. Geração de chave de cifragem
3. Cifragem dos dados

Algoritmos

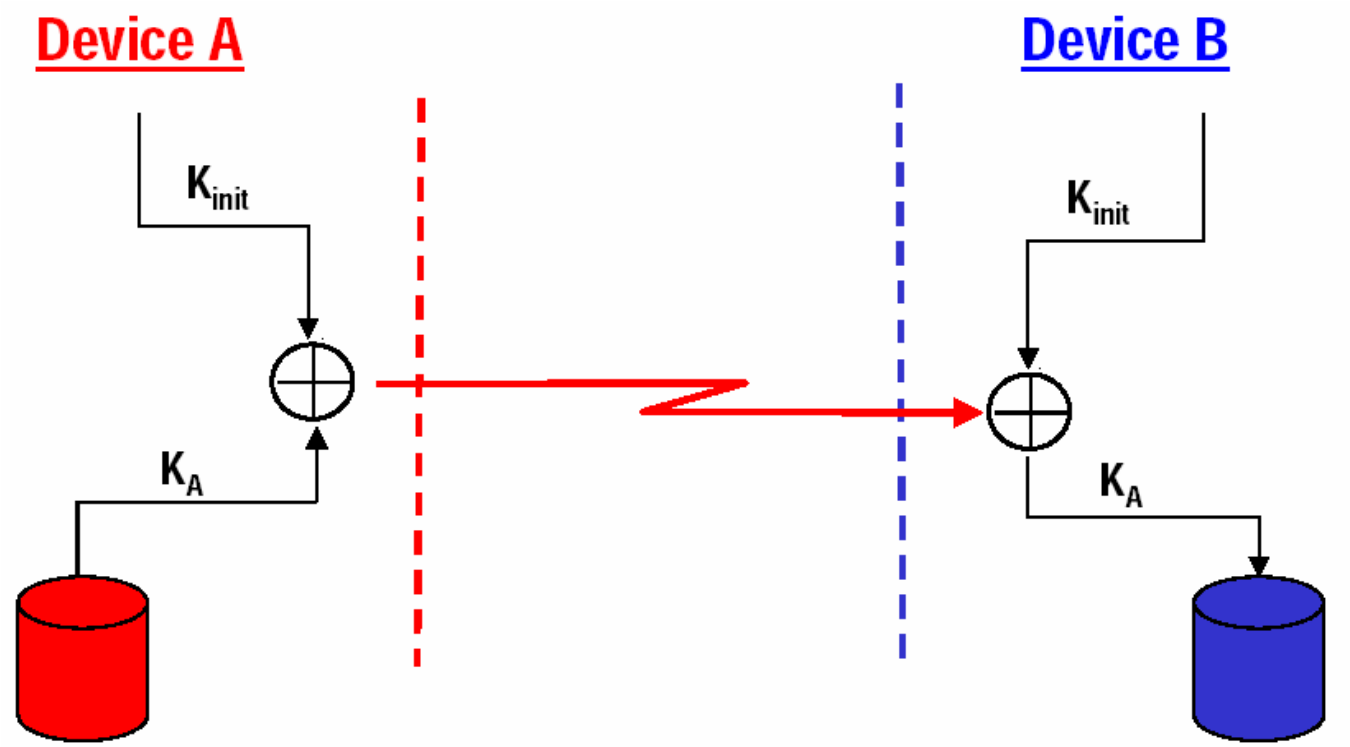
- E0 ➔ cifragem/decifragem (confidencialidade e integridade)
- E1 ➔ autenticação
- E2 ➔ geração e troca de chaves de ligação
- E3 ➔ geração e troca de chaves de cifragem

Geração da chave de inicialização (K_{init})



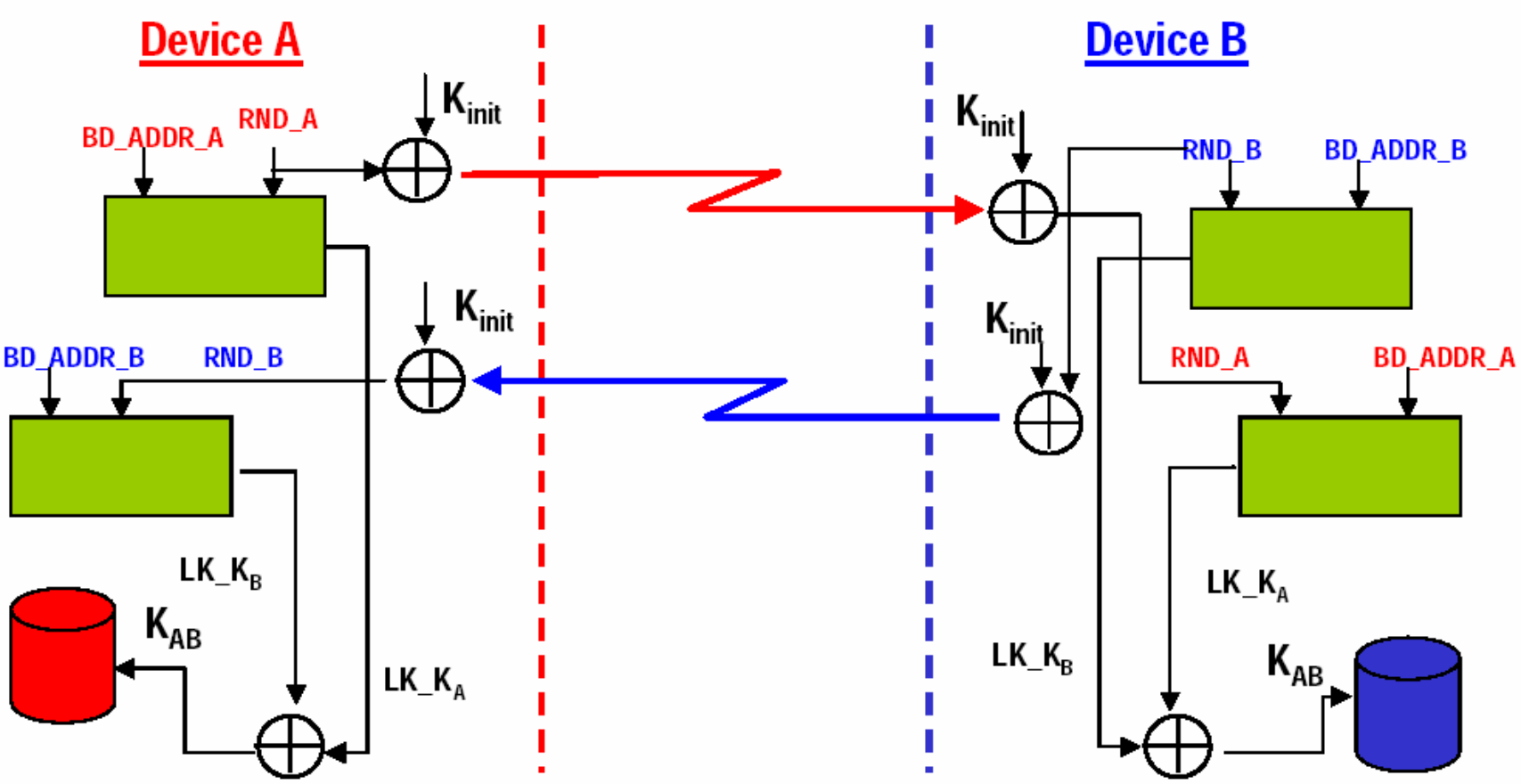
Troca de uma chave de unidade

- Chave de unidade (neste caso de A) gerada previamente
- Chave de ligação de A e B = chave de unidade de A (K_A)



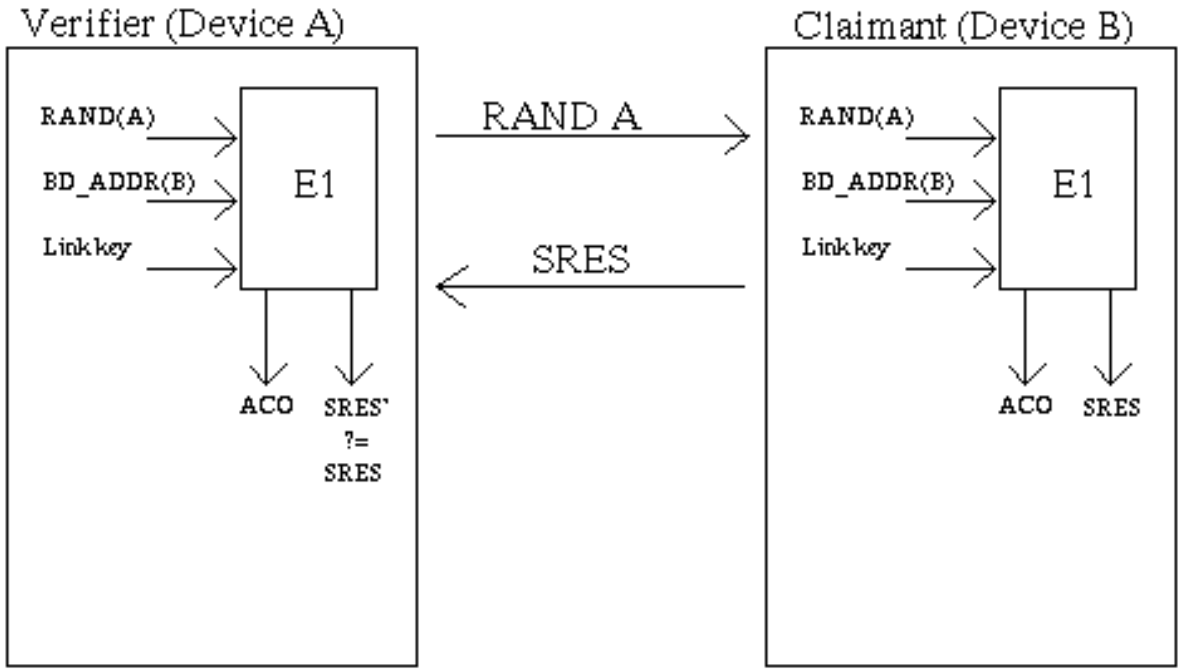
Geração de uma chave combinada

- Chave de ligação de A e B = chave combinada (K_{AB})



Autenticação

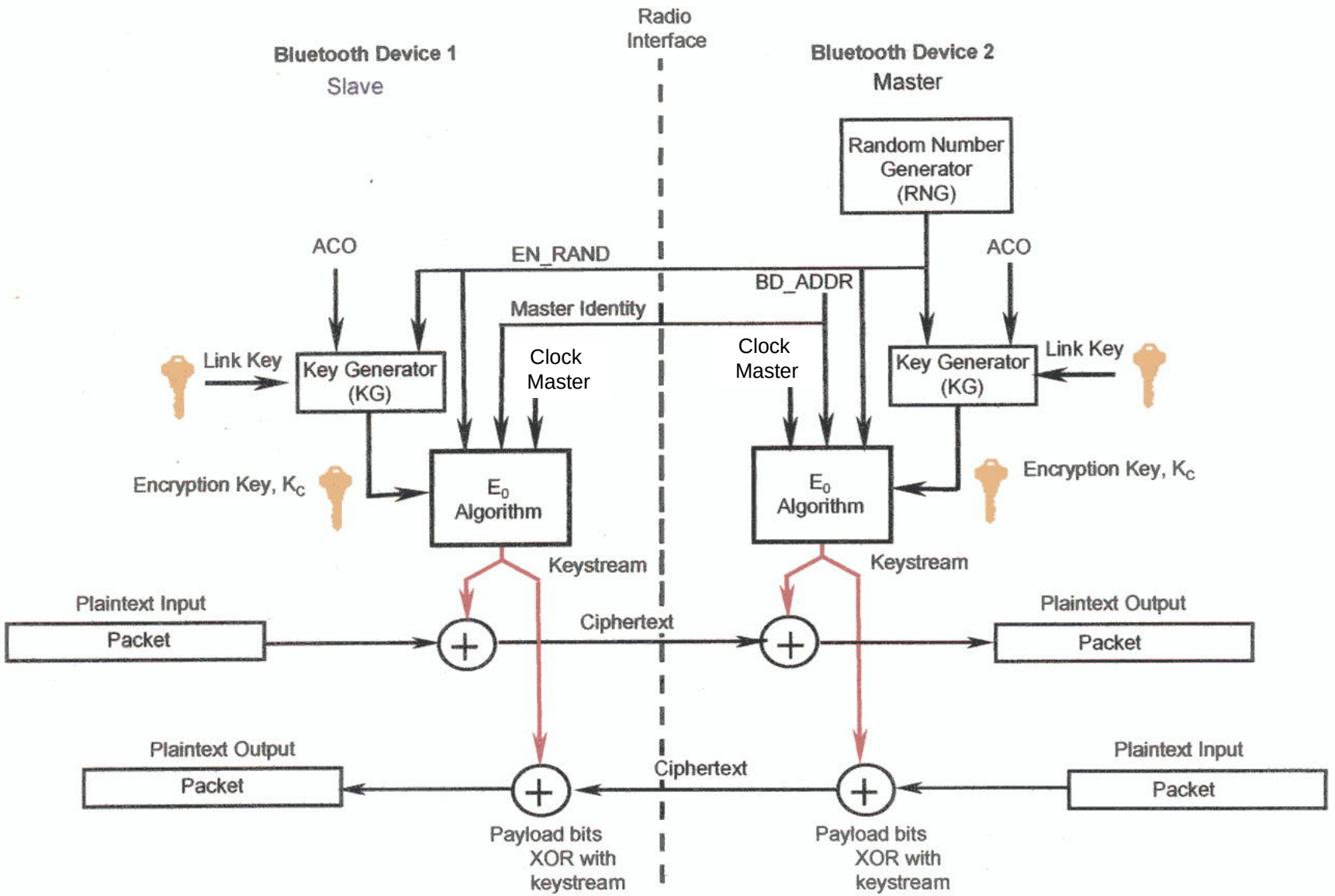
- Recurso a desafio/resposta
- Permite a um dispositivo verificar que o outro conhece a chave de ligação.



Cifragem dos dados

- Chave para cifragem (Kc) gerada a partir de uma chave de ligação, um nº aleatório (EN_RAND) e o *Authenticated Ciphering Offset* (ACO) (resultado da autenticação)
- Recurso a um algoritmo simétrico orientado ao fluxo (E0)
  - Input: Kc, EN_RAND, BD_ADDR_{MASTER}, $Clock_{MASTER}$
  - *Keystream* diferente por cada pacote ($Clock_{MASTER}$)

Cifragem dos dados



Vulnerabilidades

- À medida que as redes se tornam mais localizadas e pessoais
  - a informação transportada tende a ser mais crítica (pessoal)
    - *Telemóvel contém lista telefónica, agenda, senhas de outros sistemas, etc.*
    - *Comunicações pessoais (SMS, chamadas de voz, etc.)*
- Processo de autenticação baseado em PINs pouco cómodo
  - Cada vez que um utilizador pretende aceder a outro dispositivo → necessidade de partilhar/digitar o PIN
- Para uma maior comodidade dos consumidores (aumento das vendas) fabricantes disponibilizam muitos serviços sem qualquer autenticação/cifragem
  - Possibilidade de aceder livremente a muitos serviços críticos
  - Solução de segurança intermédia: controlo de visibilidade dos dispositivo

Vulnerabilidades (2)

- Roubo da lista telefónica de um telemóvel (T610) a partir de um PC com Linux e com um dispositivo BT normal

```
# hcitool scan
Scanning . 00:0A:D9:15:0B:1C T610-phone
# obexftp -b 00:0A:D9:15:0B:1C --channel 10 -g telecom/pb.vcf -v
Browsing 00:0A:D9:15:0B:1C ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf...\done
Disconnecting...done
```

- Alguns modelos de telemóveis permitiam(em) enviar SMSs e inicar chamadas através de commandos AT sem qualquer restrição

Vulnerabilidades (3)

- Modos de visibilidade
  - visível (*discoverable*)
  - invisível (*non-discoverable*)
    - *não envia mensagens broadcast de presença*
    - *só responde a pedidos de comunicação dirigidos ao seu endereço MAC (BD_ADDR)*
- Como contornar o modo invisível?
  - Força bruta.
    - *Primeiros 3 bytes do endereço são do fabricante. Basta saber a marca do equipamento.*
    - *O que varia são os restantes 3. Ainda assim → 2^24 possibilidades*
    - *Cada tentativa ≈ 6 s em média → demasiado tempo*
  - Por selecção
    - *Utilizadores tendem a manter rotinas → manter uma lista dos endereços conhecidos*
  - Esperar por uma comunicação. Ex: entre telemóvel e *headset*.

Vulnerabilidades (4)

- Segurança depende do PIN
  - Atacante pode apanhar tramas do "*pairing*" e praticar um ataque *offline* de dedução do PIN.
  - 16 dígitos → milhões de dias
  - 6 dígitos → ≈ 10 s
  - 4 dígitos → < 1 s

Vulnerabilidades (4)

- Vigilância (privacidade)
  - Endereço MAC é constante → identifica o proprietário do dispositivo
  - Com equipamento adequado, mesmo um dispositivo de classe 3 pode ser acompanhado a longas distâncias: > 1 km

Vulnerabilidades (5)

- Partilha de chave de unidade pode levar à escuta de comunicações