

# **Identificação Digital**

Apêndice B da Apostila

**Criptografia e Segurança na Informática**

**Maio de 2004**

Prof. Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

# O que é identificação?

Parece óbvia a resposta,  
donde o perigo.

Principalmente no mundo dos bits!

# Identidade

Id

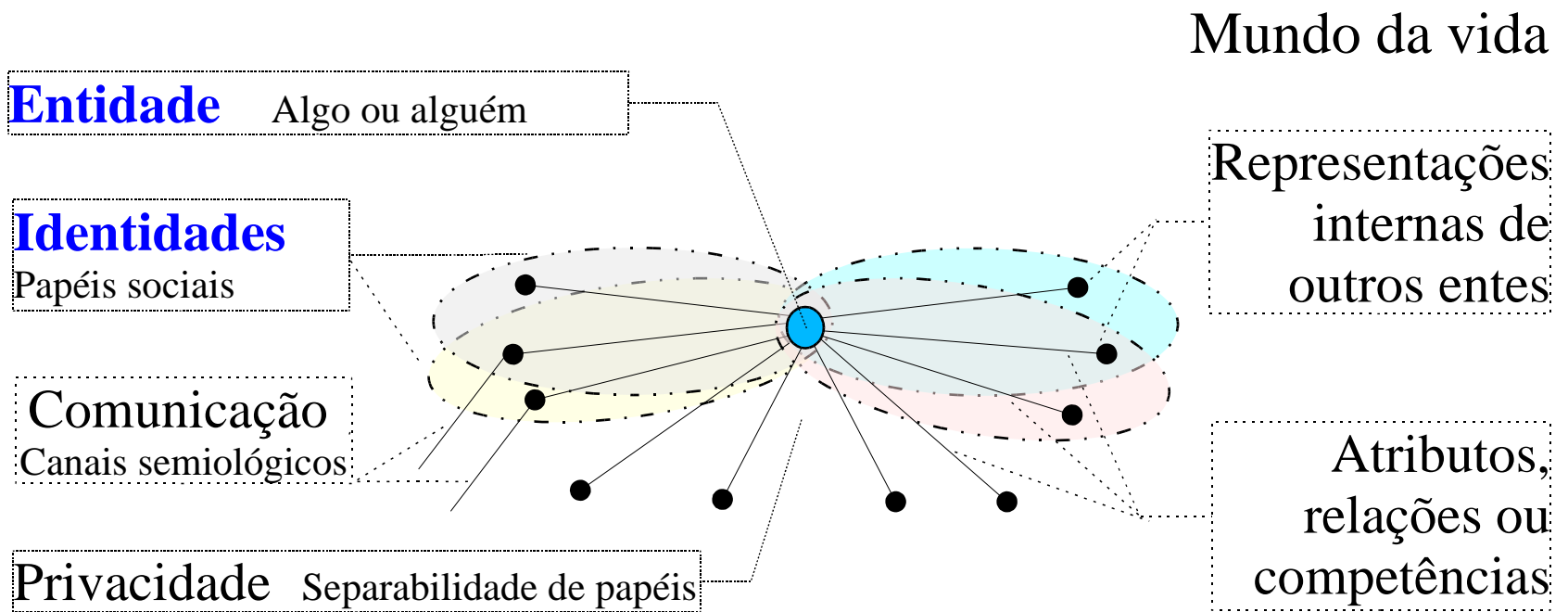
do latim *isto, este*

+

Entidade:

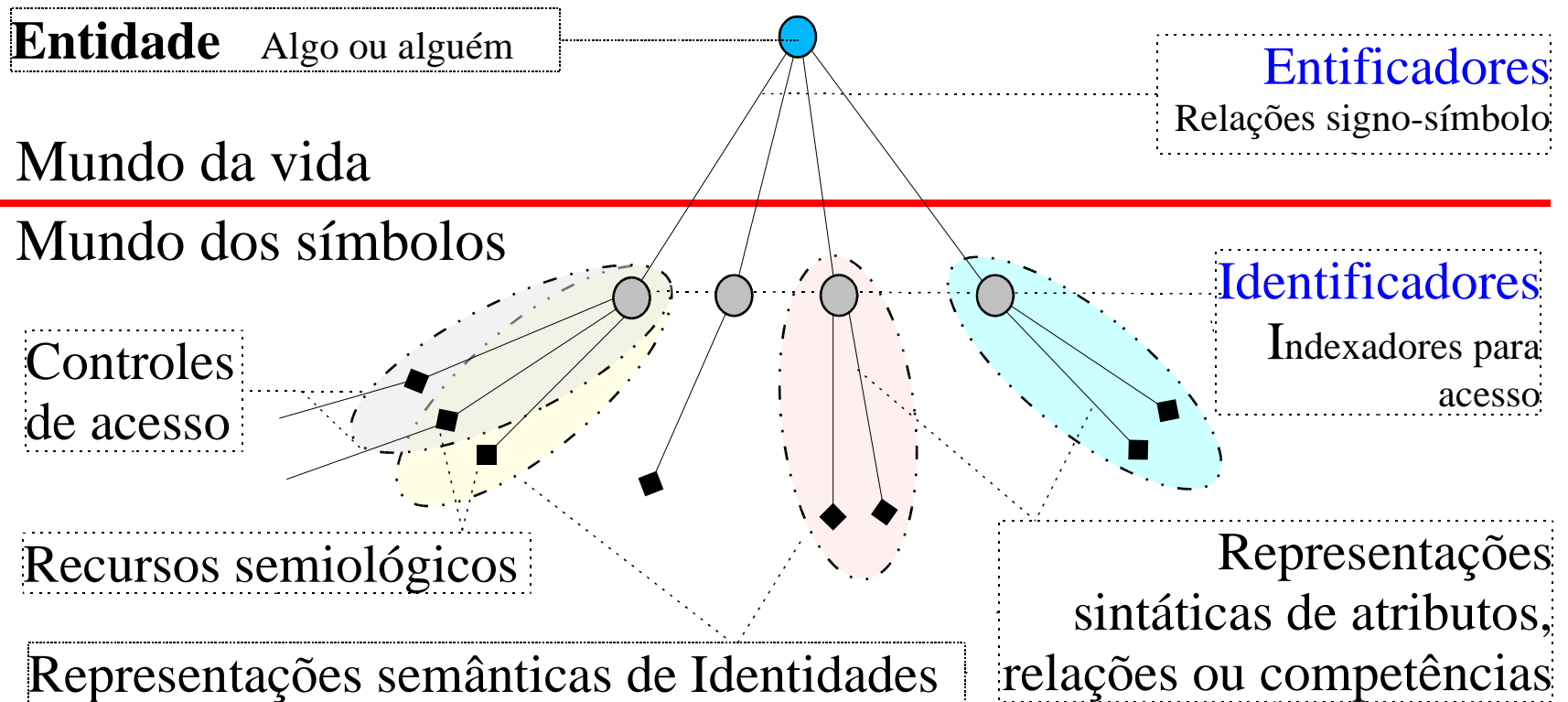
*ente, ser, o que existe,  
o que é, coisa, objeto*

# Semiologia da identidade

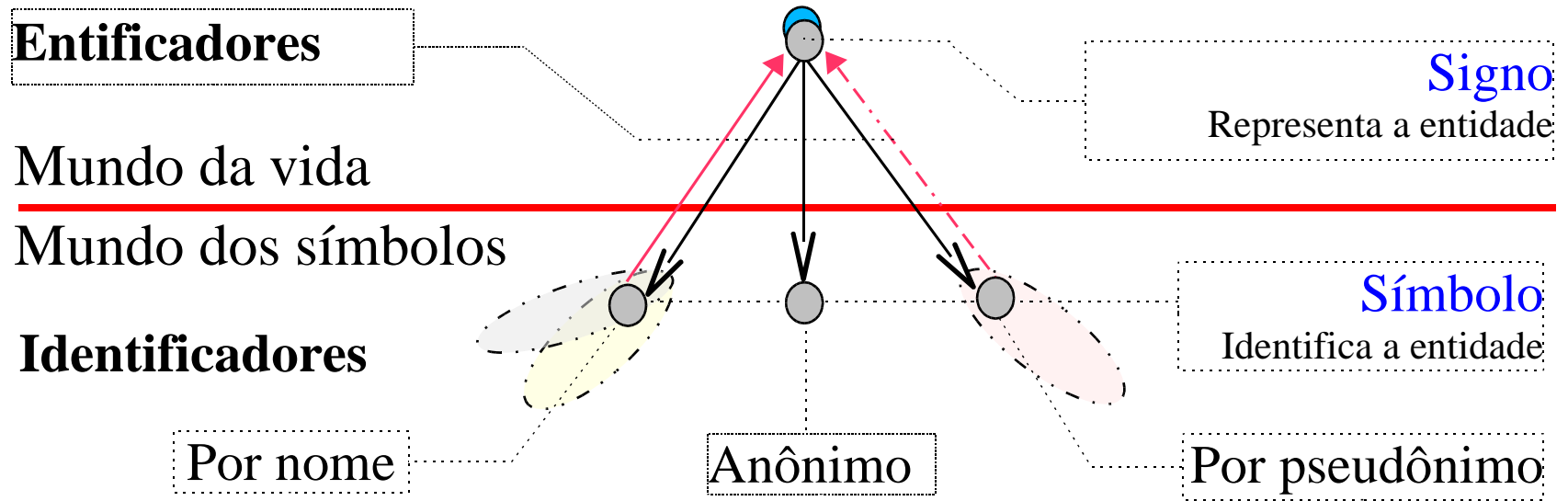


Adaptado de Roger Clarke, Australian National University

# Identificação digital



# Tipos de identificação digital



Pseudônimo : Relação símbolo -> signo de difícil conhecimento ( ·····→ )

Anônimo : Relação desconhecida (para entidades que não a representada)

# Tipos de entificadores

Marcas, atos ou sinais (signos)  
aptos a simbolizar uma identidade

**T1-** O que só o ente pode **dizer** (deve saber)

*Ex: Senha “secreta”, chave privada*

# Tipos de entificadores

Marcas, atos ou sinais (signos)  
aptos a simbolizar uma identidade

**T1-** O que só o ente pode dizer (deve saber)

*Ex: Senha “secreta”, chave privada*

**T2-** O que só o ente pode **fazer** (sabe produzir)

*Ex: Assinatura de punho, timbre de voz*



# Tipos de entificadores

Marcas, atos ou sinais (signos)  
aptos a simbolizar uma identidade

**T1-** O que só o ente pode dizer (deve saber)

*Ex: Senha “secreta”, chave privada*

**T2-** O que só o ente pode fazer (sabe produzir)

*Ex: Assinatura de punho, timbre de voz*

**T3-** O que só o ente pode **mostrar** (tem para usar)

*Ex: Marca biométrica, fisionomia, token*

# Modos de entificação

**M1- Apresentação:** Instauração de entificador

*Modo de se conhecer algo ou alguém*

**M2- Identificação:** Validação de entificador

*Modo de se convencer do reconhecimento de algo ou alguém*

**M3- Autenticação:** Comprovação de entificador

*Modo de convencer outrem do reconhecimento de algo / alguém*

**M4- Assinatura:** Autenticação p/ repres. vontade

*Modo de convencer outrem do reconhecimento de algo que representa uma manifestação de vontade de alguém*

# Mecanismos básicos de proteção

## **B1- Controle de Acesso:**

*Para legitimidade na identificação  
de agentes de transações em sistemas fechados*

# Mecanismos básicos de proteção

## **B1-** Controle de Acesso:

*Para legitimidade na identificação de agentes de transações*

## **B2-** Cifragem (criptografia):

Transação para sigilo

*Na comunicação entre agentes que se identificam mutuamente*

# Mecanismos básicos de proteção

## **B1- Controle de Acesso:**

*Para legitimidade na identificação de agentes de transações*

## **B2- Cifragem (criptografia):** Transação para sigilo

*Na comunicação entre agentes identificados*

## **B3- Autenticação:** Cifragem para integridade

*De identificadores e conteúdos comunicados  
entre agentes identificados*

# Mecanismos básicos de proteção

## **B1- Controle de Acesso:**

*Para legitimidade na identificação de agentes de transações*

## **B2- Cifragem (criptografia):** Transação para sigilo

*Na comunicação entre agentes identificados*

## **B3- Autenticação:** Cifragem para integridade

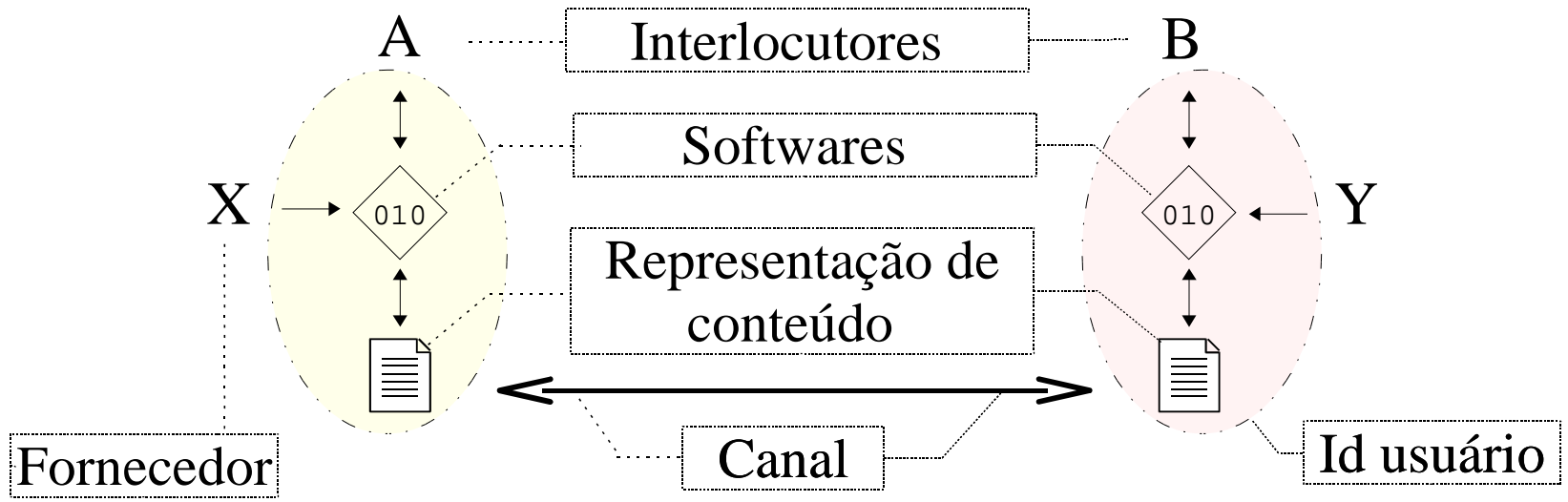
*De identificadores e conteúdos comunicados*

## **B4- Certificação:** Autenticação recursiva

*Para legitimidade de identificadores em redes abertas*

# Modos de comunicação digital

Conforme **Representação** de conteúdo



Padrão **fechado** : Fornecedores de software  $X = Y$  ( relacionados negocialmente )

Padrão **aberto** :  $X, Y$  podem concorrer ( relacionados semiologicamente )

# Modelos de segurança

Conforme **Interesses** conflitantes envolvidos

**I1-**

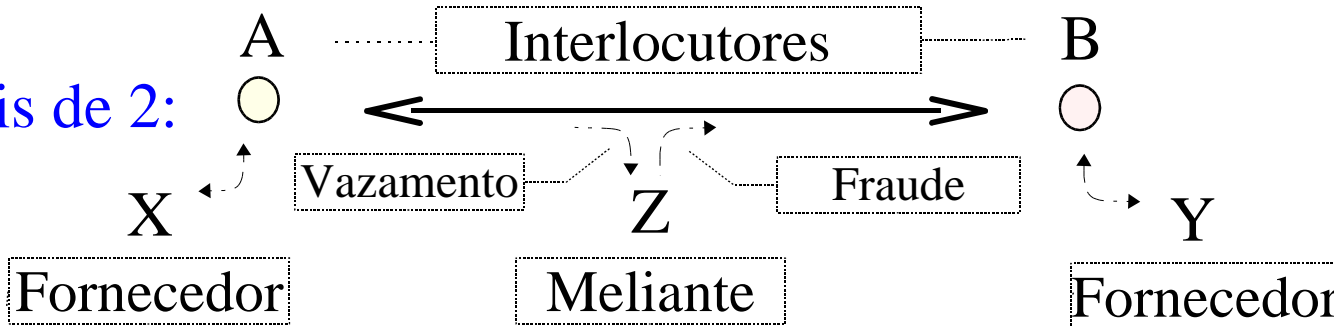
Até 2:



IA = IB ou  
IA = I? ou  
IB = I?

**I2-**

Mais de 2:



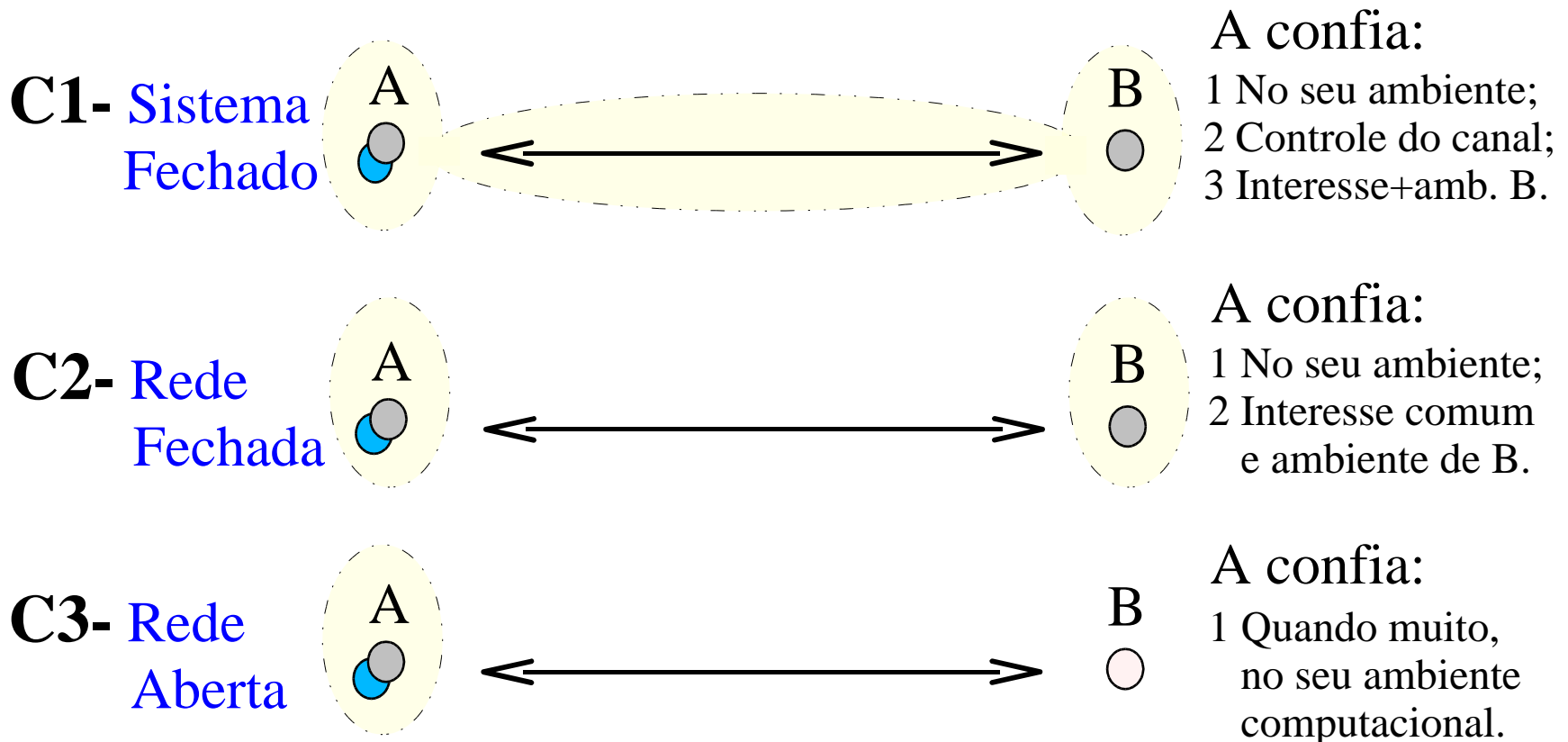
Safety = proteção contra Murphey

**Security** = proteção contra HMD



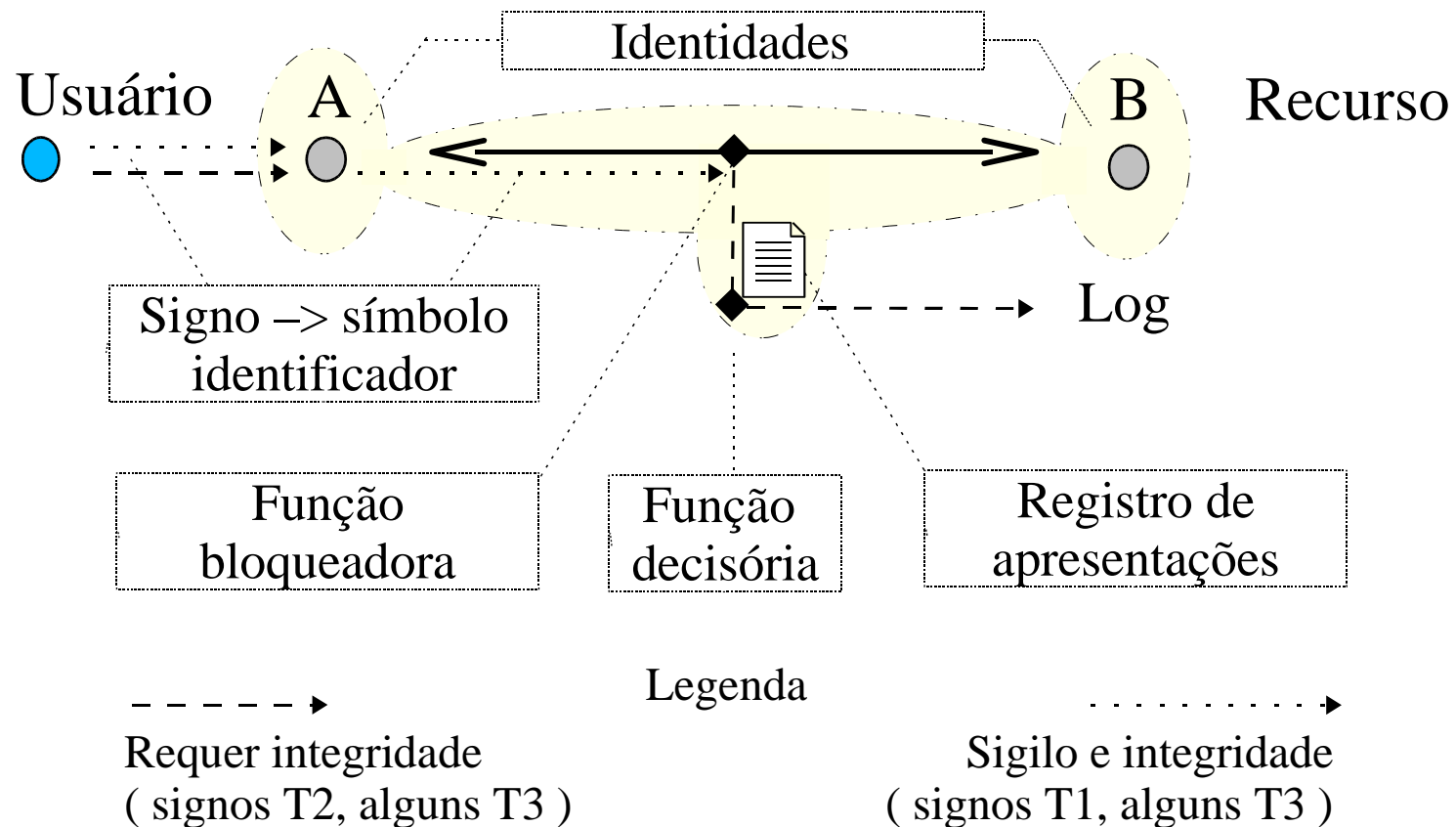
# Modelos de segurança

Conforme premissas de **Confiança** envolvidas



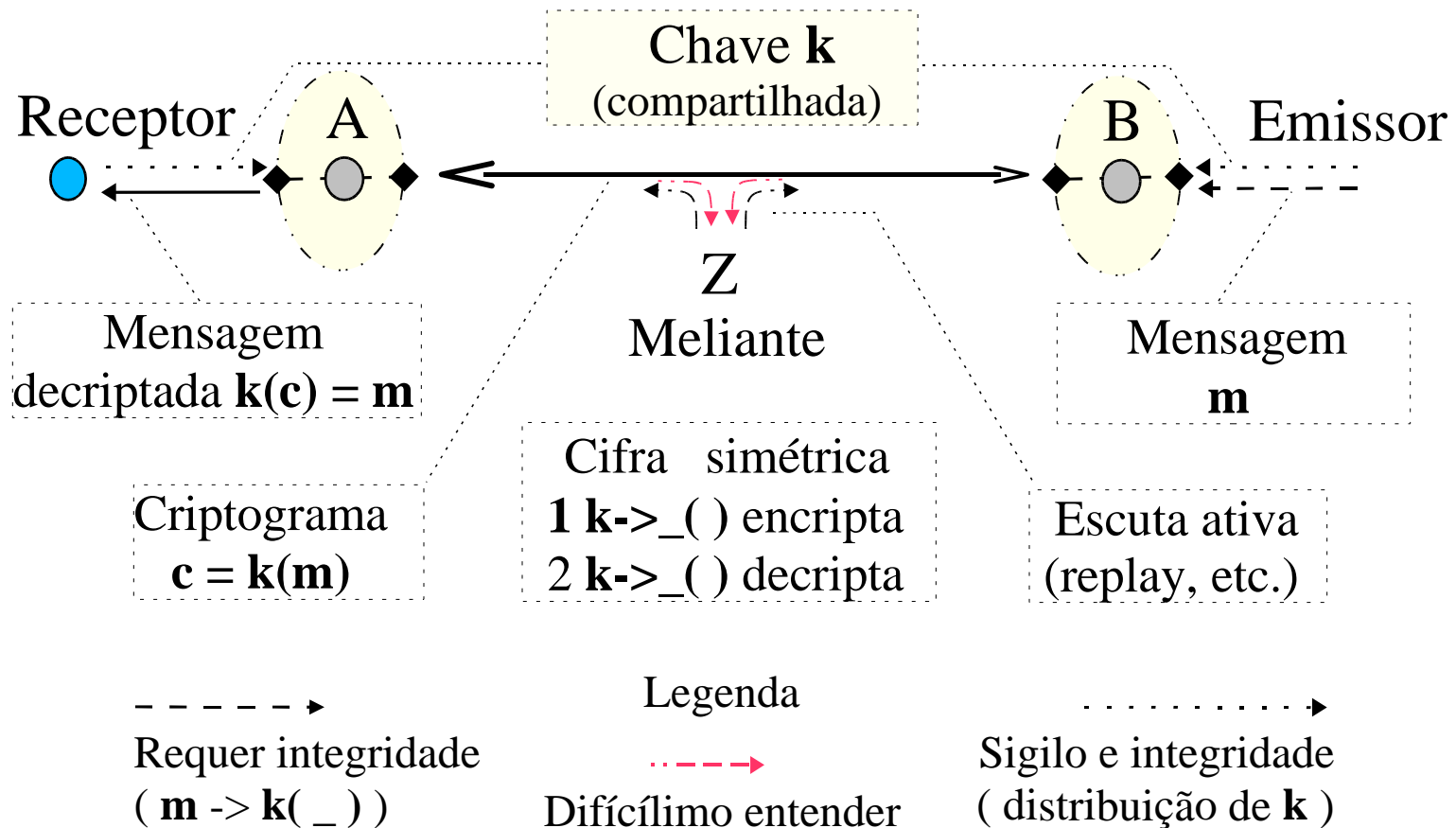
# Segurança digital - Safety

Mecanismo básico **B1- controle de acesso** em C1:



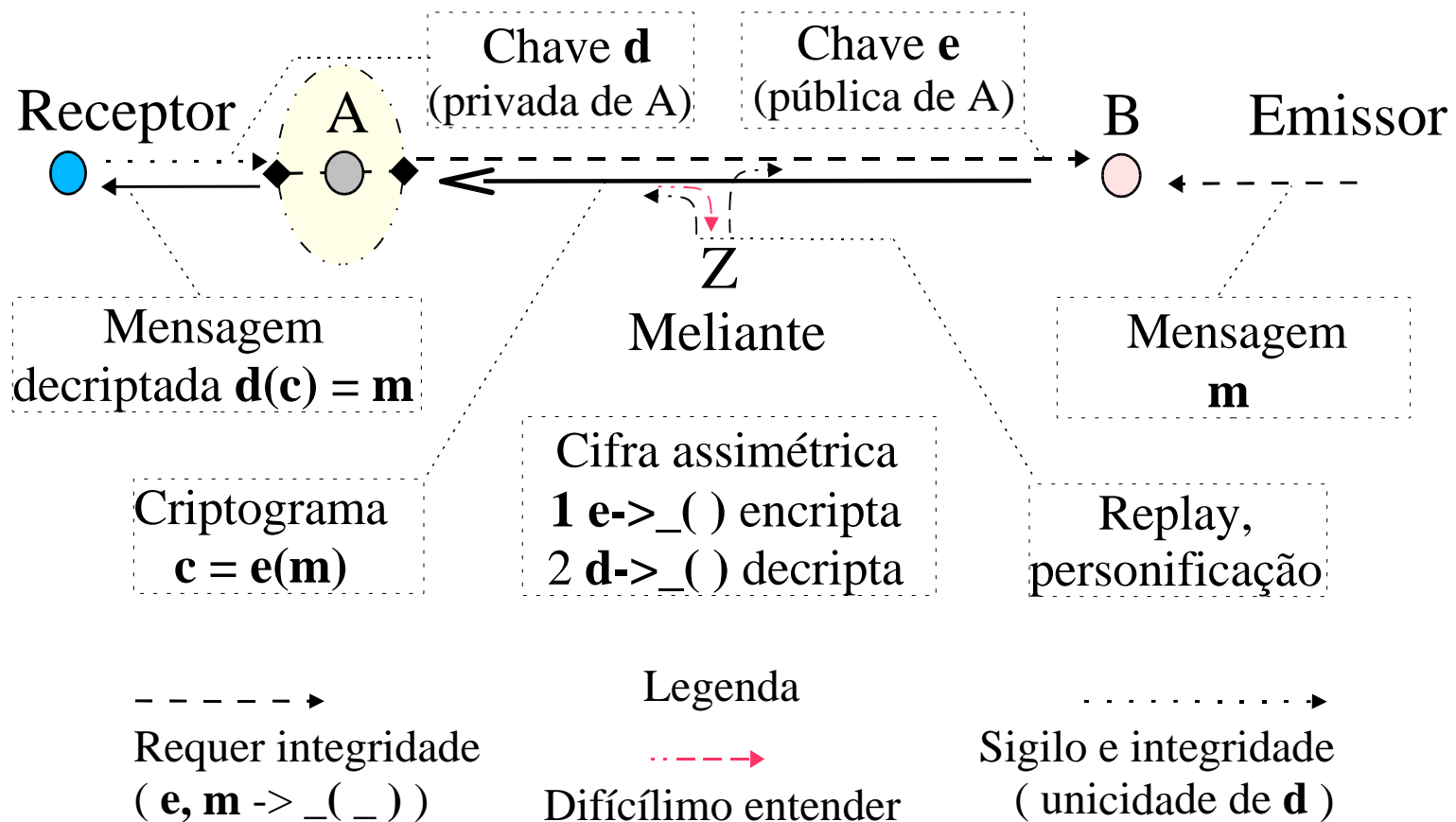
# Segurança digital - Safety

Mecanismo básico B2 - sigilo p/ acesso remoto em C2:



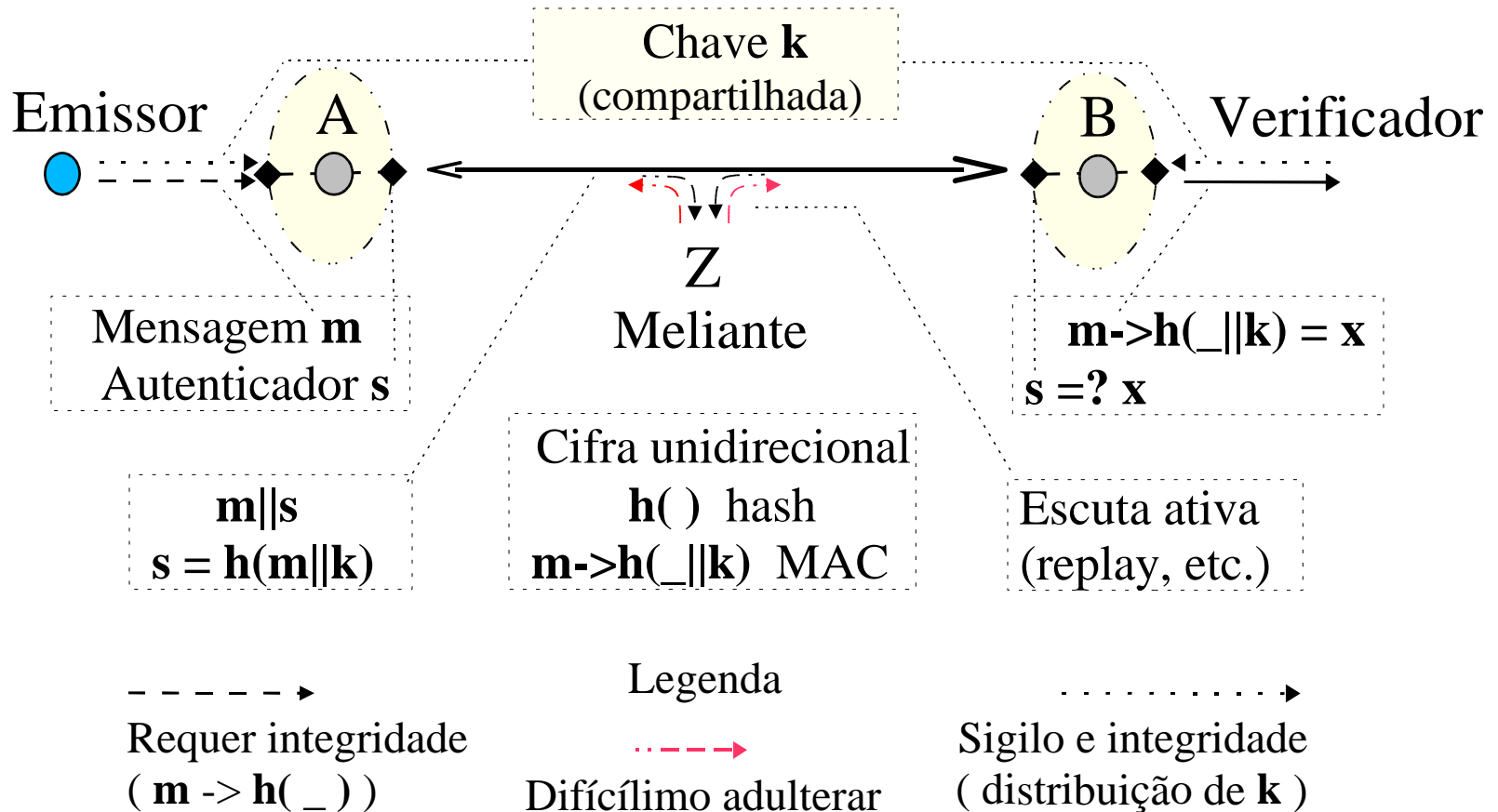
# Segurança digital - Safety

Mecanismo básico B2 - sigilo p/ acesso remoto em C3:



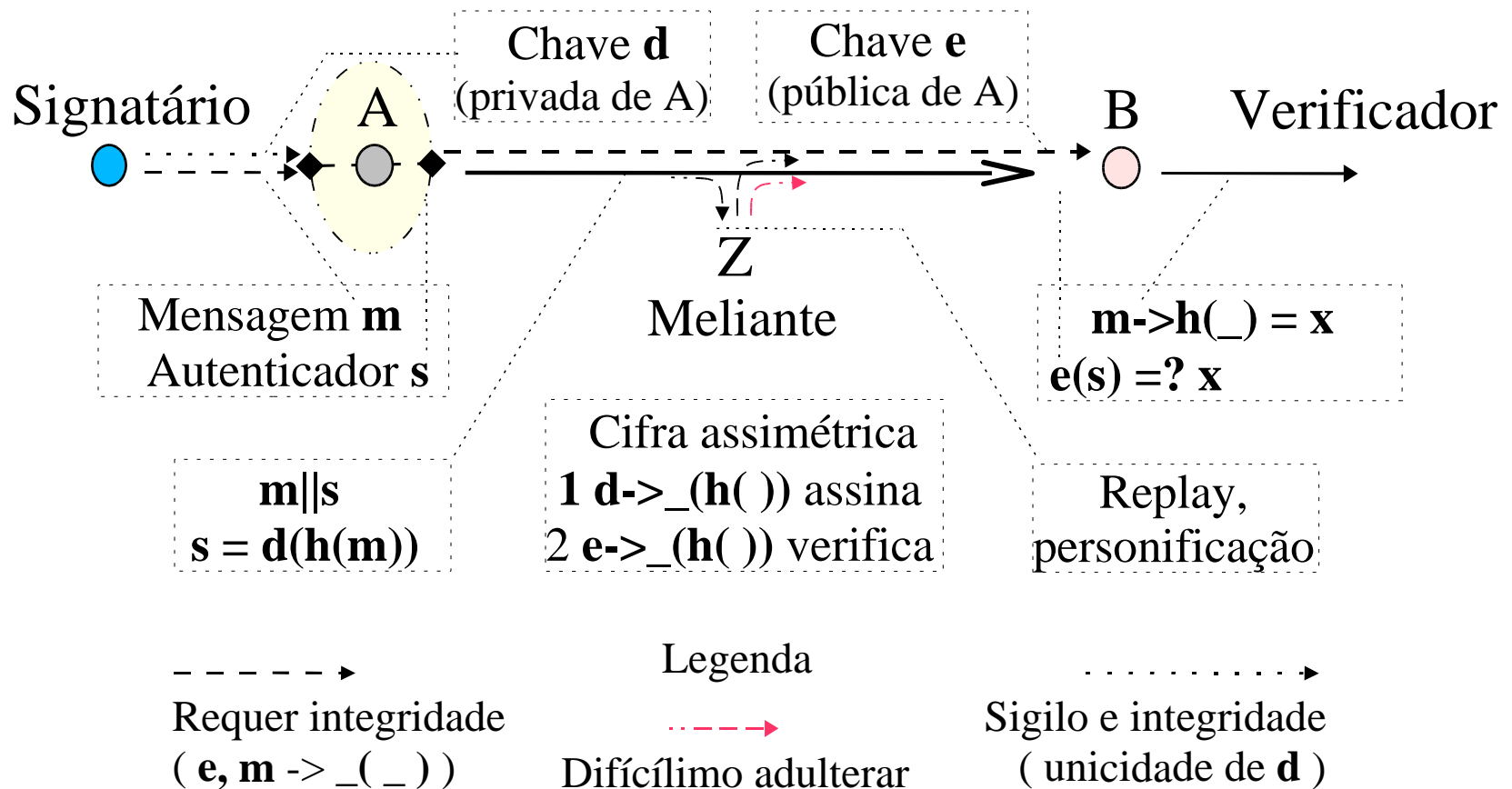
# Segurança digital - Safety

## Mecanismo básico B3 - integridade em C2: MAC



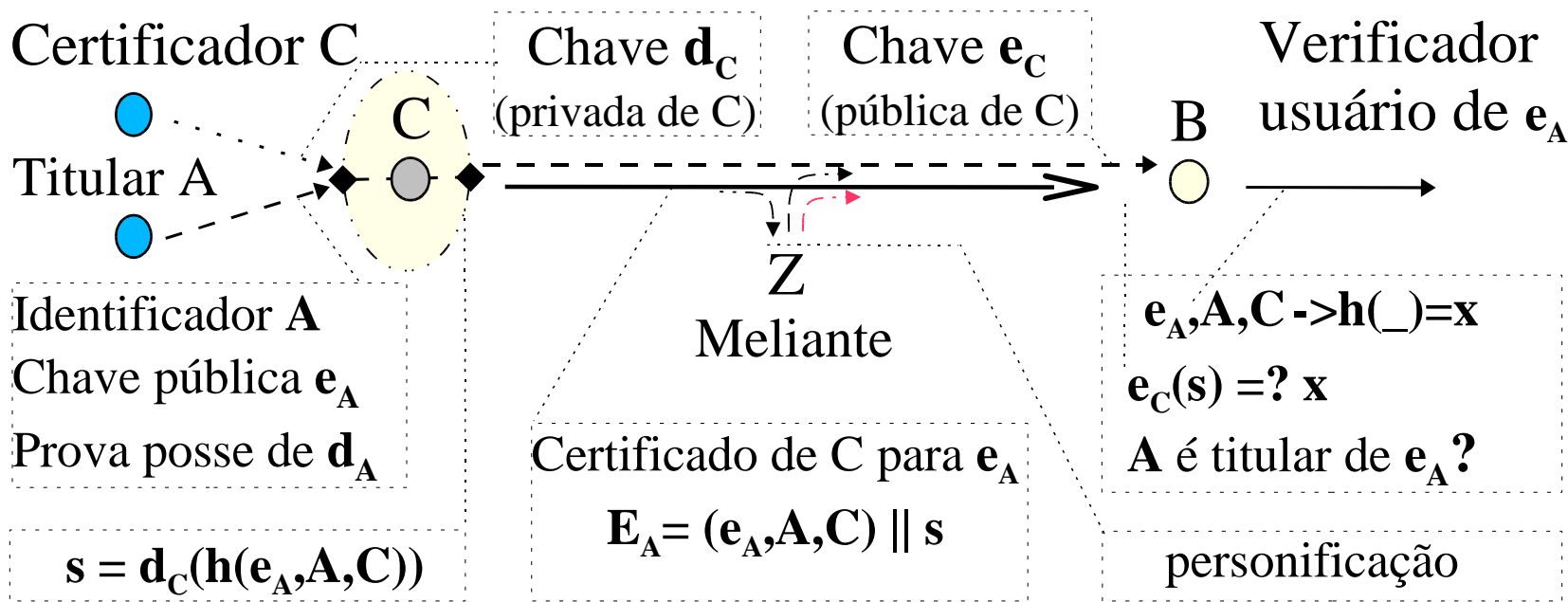
# Segurança digital - Safety

Mecanismo básico **B3** - integridade em C3: assinatura



# Segurança digital - Safety

## Mecanismo básico **B4** - integridade em C3: certificação



- >  
Requer integridade  
(  $e_A, A \rightarrow E_A$  )
- Legenda  
- - - - ->  
Difícilimo adularar
- .....>  
Sigilo e integridade  
( unicidade  $d_A, d_C$  )