Identificação Digital

Academia Nacional da Polícia Federal

Maio de 2004

Prof. Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

pedro.jmrezende.com.br/sd.php

O que é identificação?

Parece óbvia a resposta,
donde o perigo.

O que é identificação?

Parece óbvia a resposta,
donde o perigo.

Principalmente no mundo dos bits!

Identidade

Idem:

do latim *o mesmo*

Identidade

Idem

do latim *o mesmo*

+

t id ade:

do latim isto, este

Semiologia da identidade

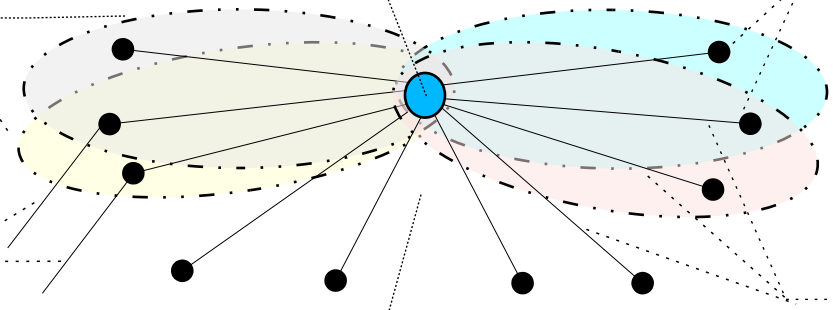
Mundo da vida

Entidade Algo ou alguém

Identidades
Papéis sociais

Comunicação
Canais semiológicos

Privacidade Separabilidade de papéis

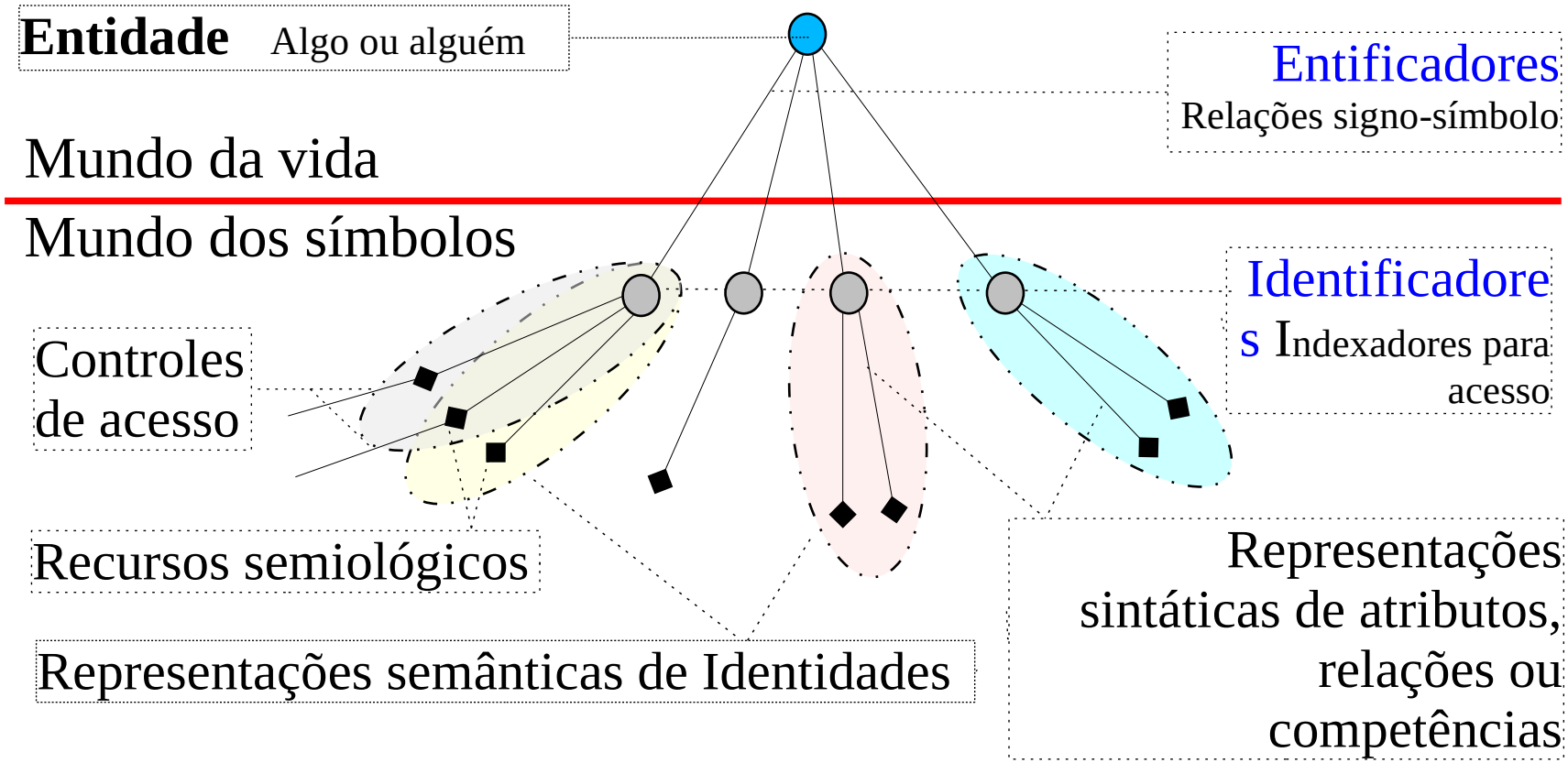


Representaçõe s internas de outros entes

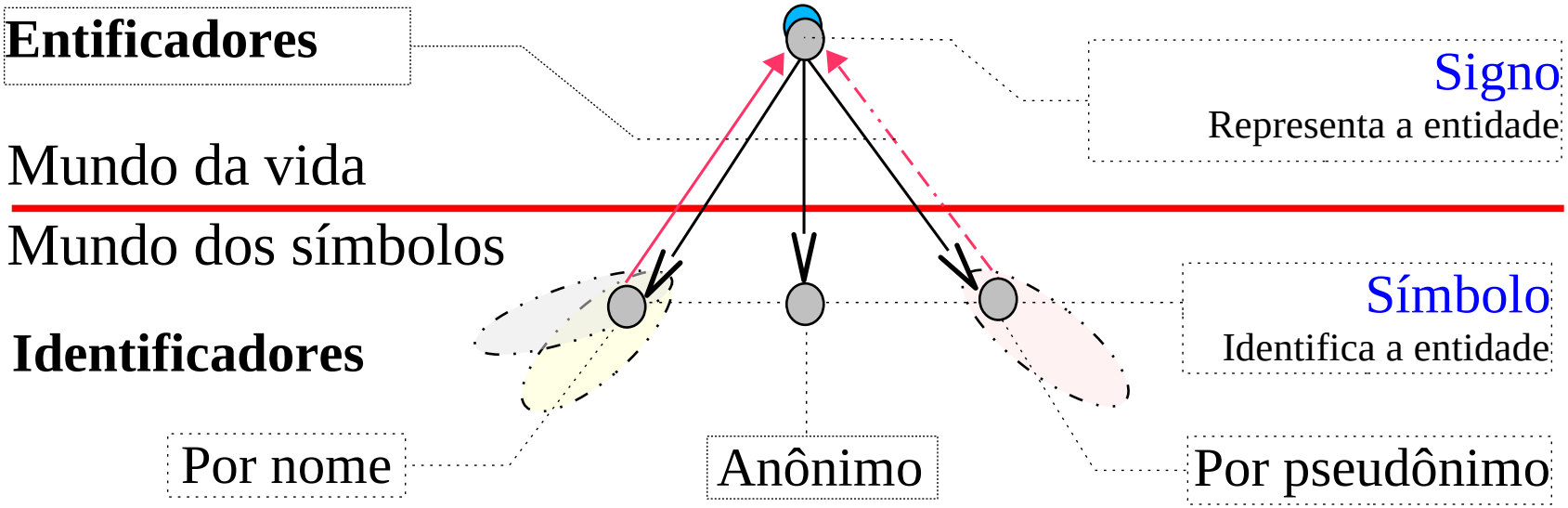
Atributos, relações ou competências

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

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

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 ou alguém

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

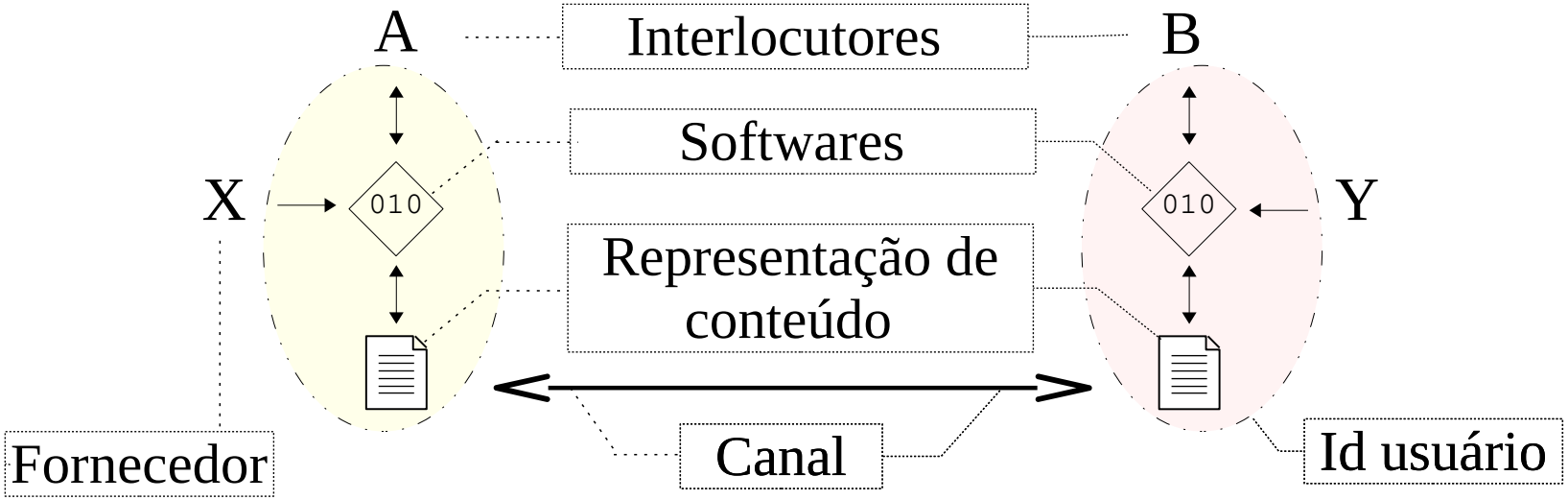
De identificadores e conteúdos comunicados

B4- Certificação: Autenticação recursiva

Para legitimidade de identificadores em redes abertas

Modos de comunicação digital

Conforme Representação de conteúdo

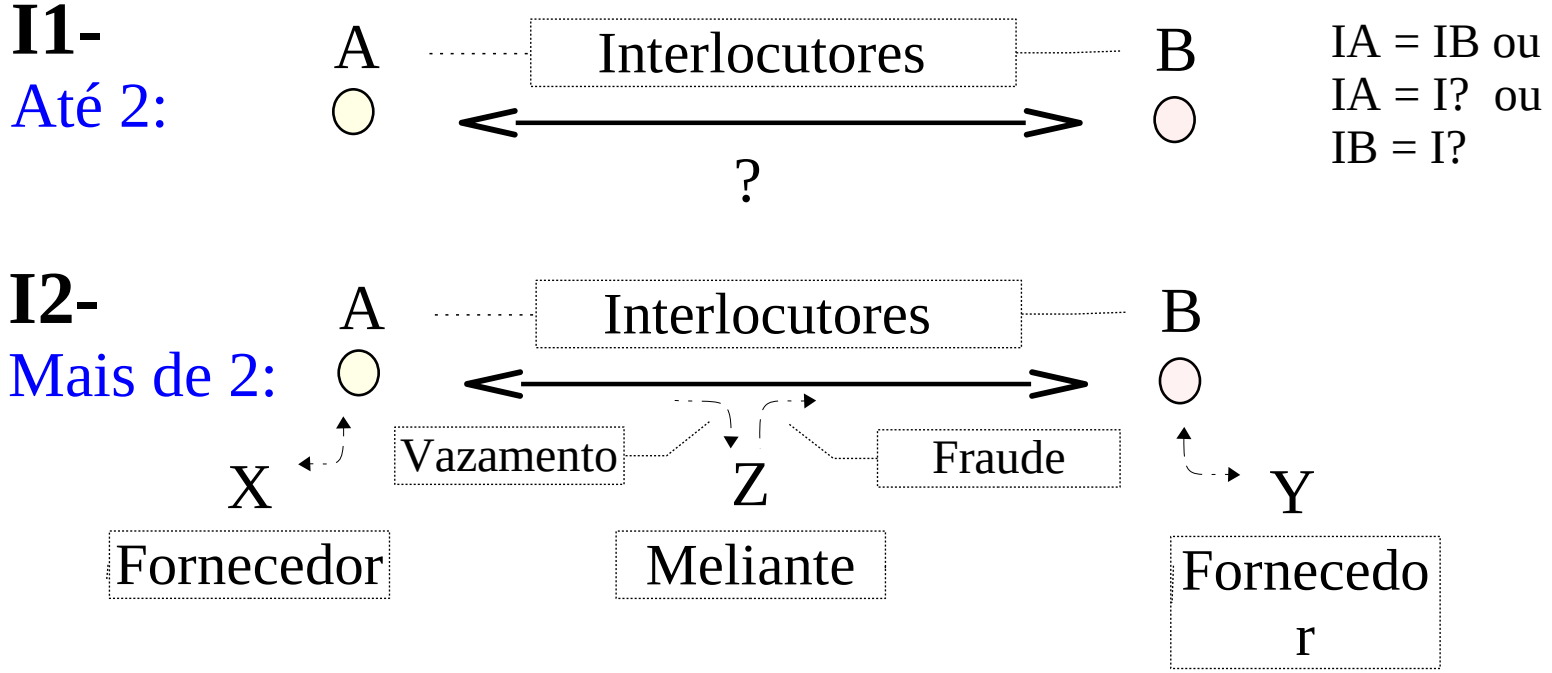


Padrão fechado : Fornecedores de software X = Y (relacionados negocialmente)

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

Modelos de segurança

Conforme Interesses conflitantes envolvidos



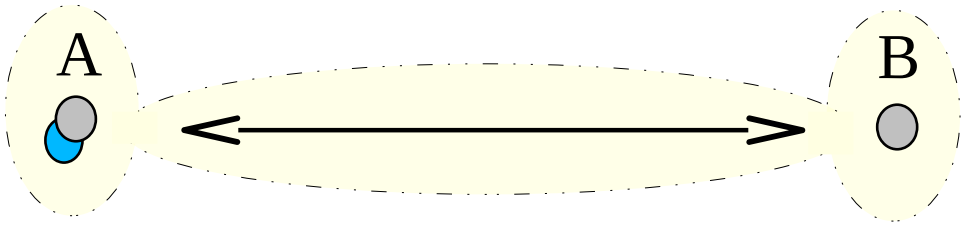
Safety = proteção contra Murphey

Security = proteção contra HMD

Modelos de segurança

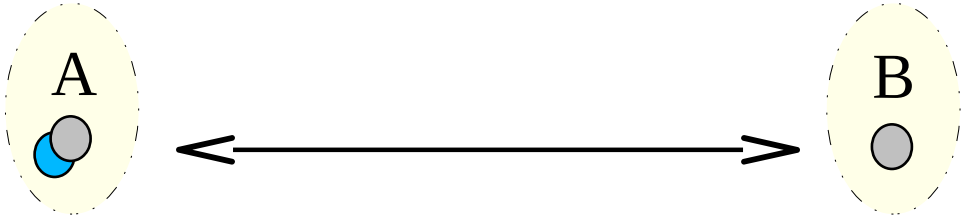
Conforme premissas de Confiança envolvidas

C1- Sistema Fechado



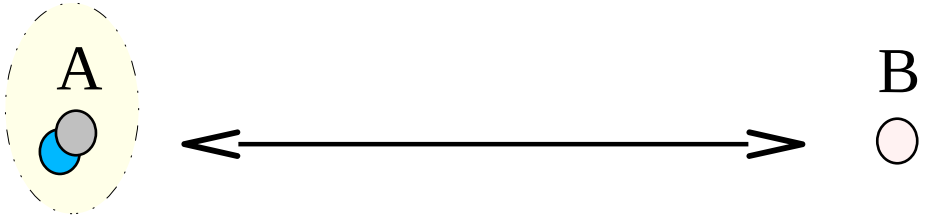
A confia:
1 No seu ambiente;
2 Controle do canal;
3 Interesse+amb. B.

C2- Rede Fechada



A confia:
1 No seu ambiente;
2 Interesse comum e ambiente de B.

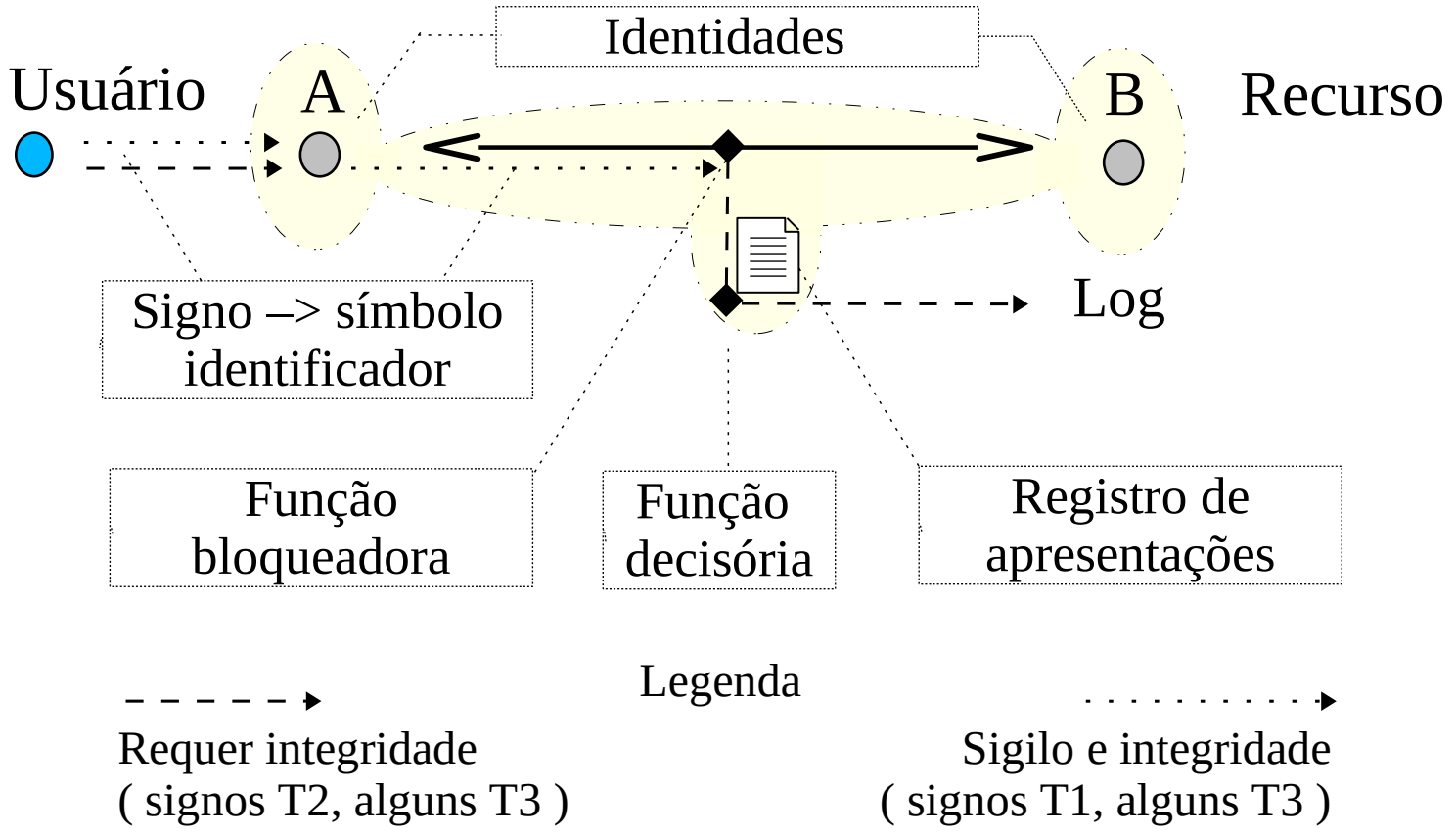
C3- Rede Aberta



A confia:
1 Quando muito, no seu ambiente computacional.

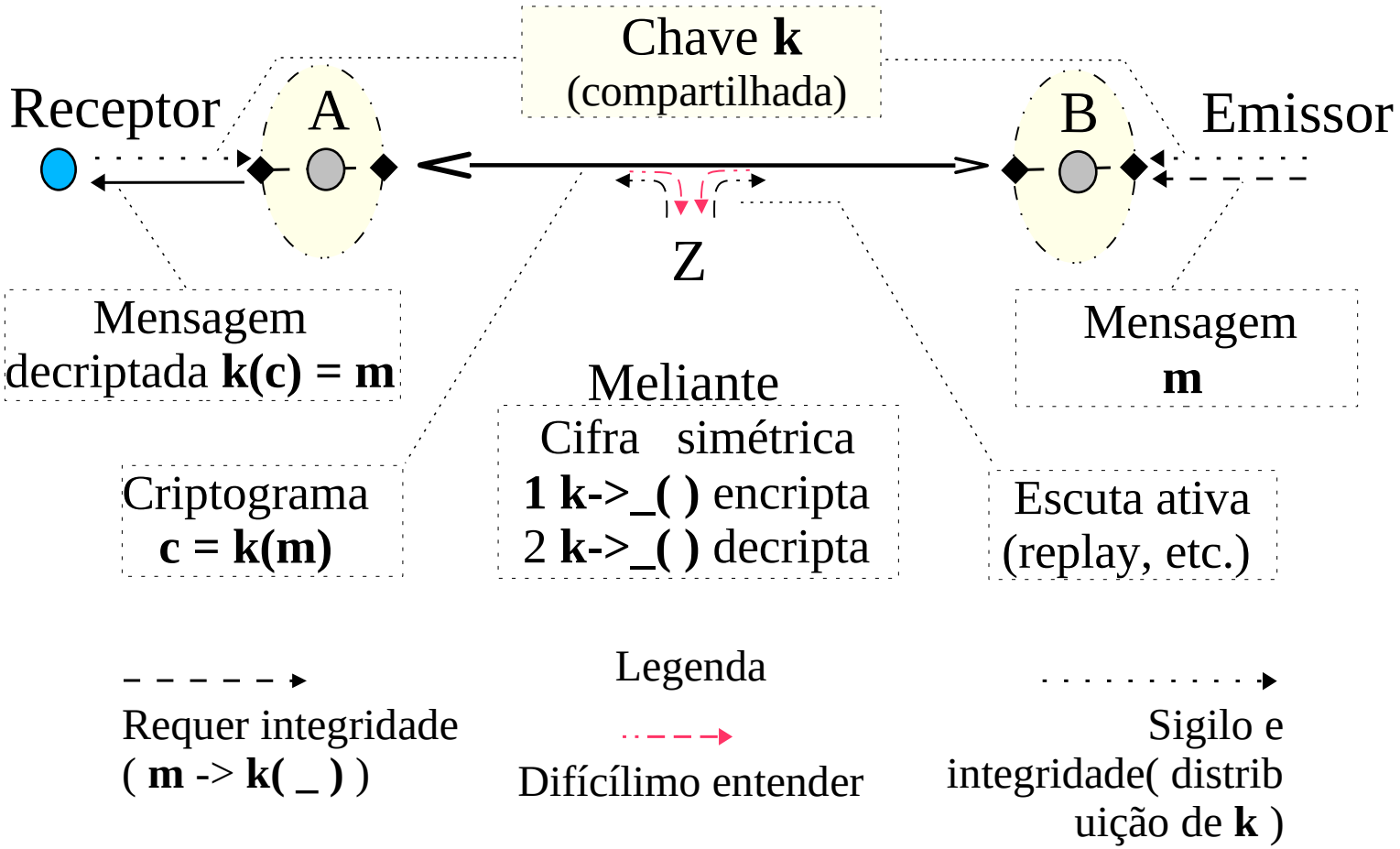
Segurança digital - Safety

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



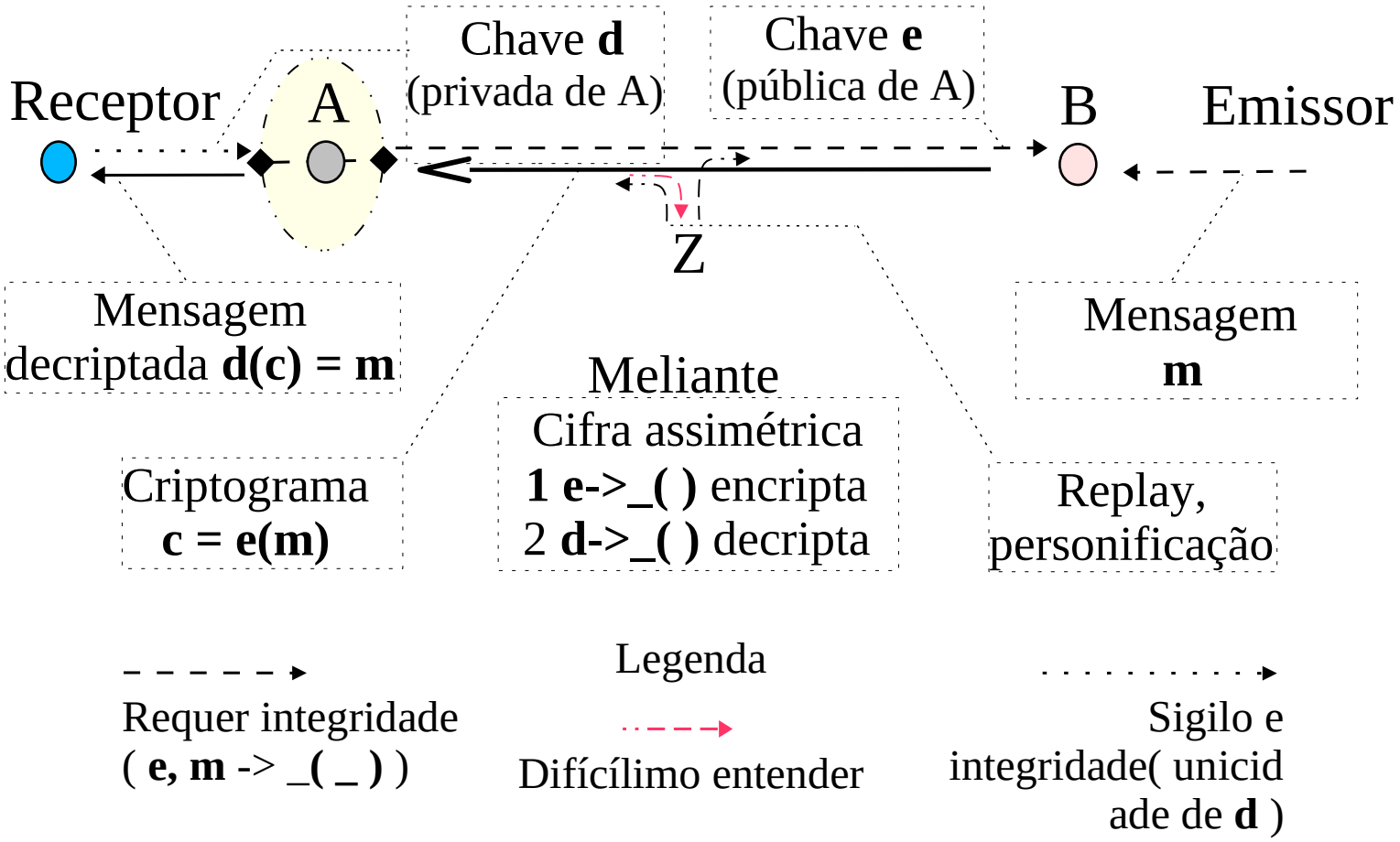
Segurança digital - Safety

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



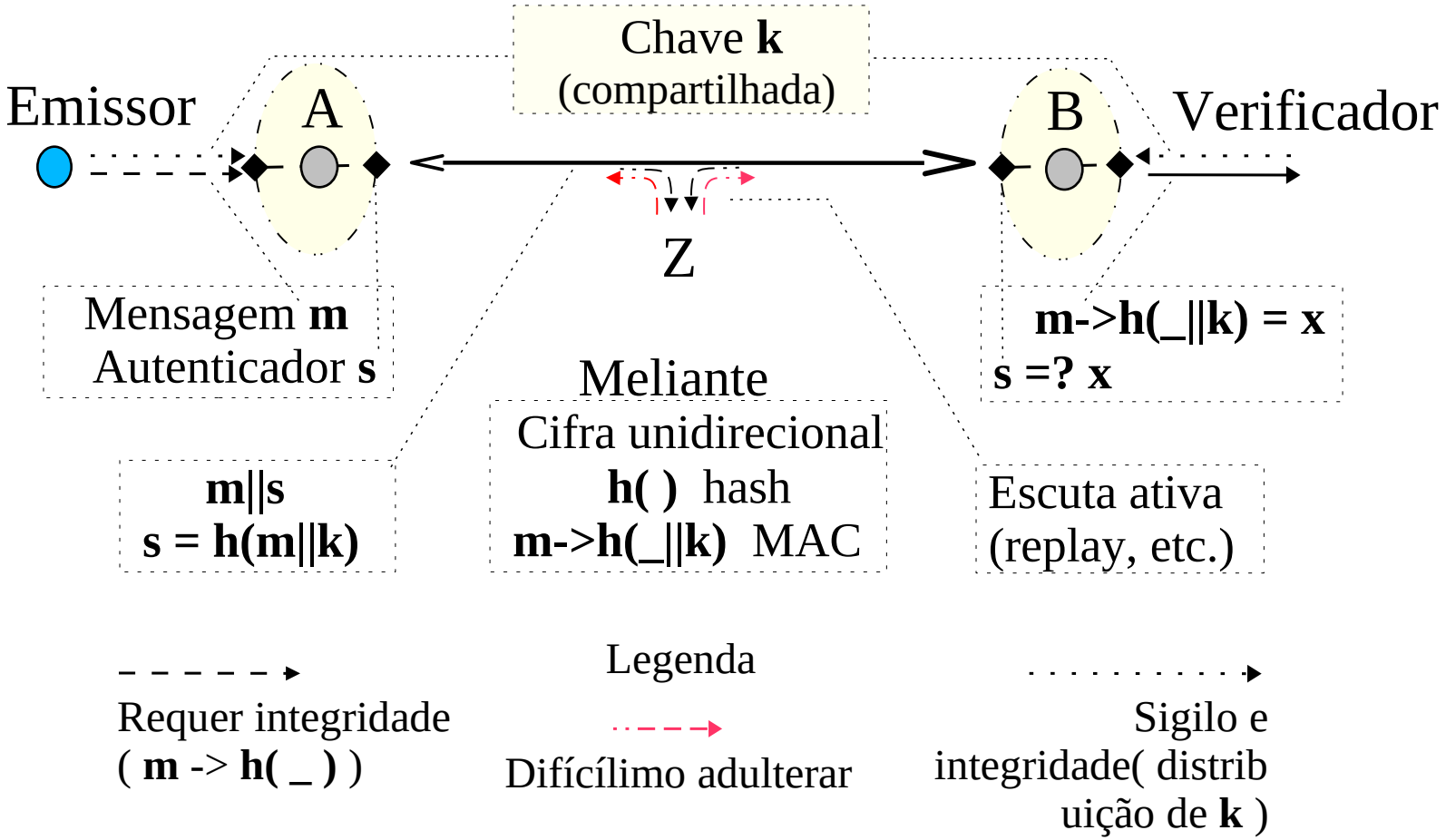
Segurança digital - Safety

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



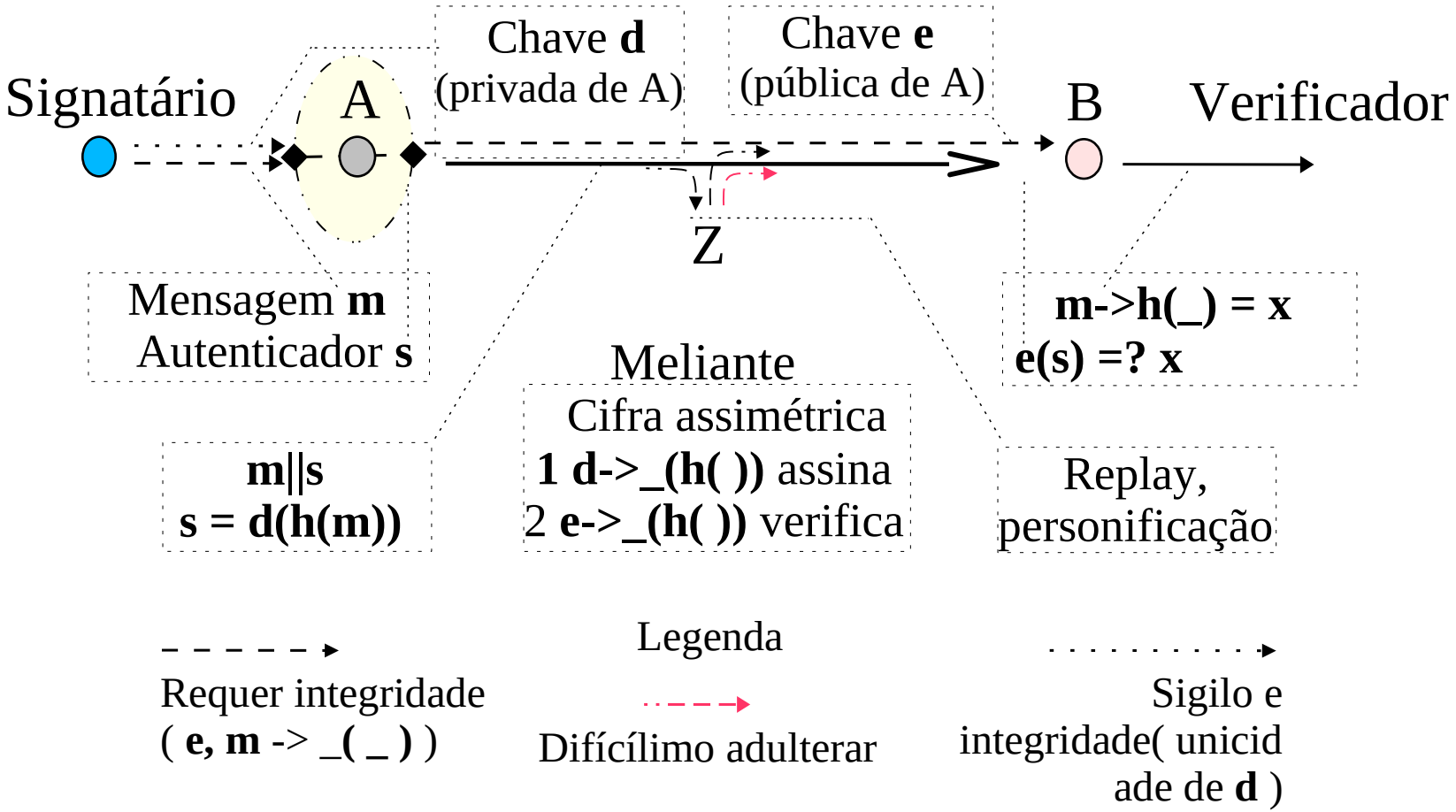
Segurança digital - Safety

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