Segurança computacional
Segurança “de dados”

Preliminares

Pedro A .D. Rezende
UnB – Ciência da Computação

V. 31.03.2019

Segurança computacional

Preliminares

Noções fundamentais

1. Noção de Segurança: Sentimento ou processo?
2. O que é Comunicação segura? E Criptografia?
3. O que são, e como se produzem significados?
4. Processos de segurança em contextos virtuais

Marcas gráficas

Conceito a definir adiante *Destaque* **Conceito sendo definido**

Definição ou Explicação Risco Referencial de interesse

Segurança computacional

Expectativa inicial?

Segurança computacional

Perspectiva final

1. Noção de Segurança

O que significa isso?

1. Segurança, interesses e impasses

Possibilidades de divergência de interesses entre

- os que desenvolvem e fornecem tecnologias digitais,
- os que precisam de proteção contra uso indevido destas,
- os que competem entre si por um desses objetivos,
- os que fazem isso/aquilo por meios ou para fins escusos,

induzem impasses e conflitos que se tornam elementos cada vez mais cruciais nos *processos de segurança* relativa a informação, comunicação, dados ou computação.

1. Segurança, interesses e impasses

Possibilidades de divergência de interesses entre

- os que desenvolvem e fornecem tecnologias digitais,
- os que precisam de proteção contra uso indevido destas,
- os que competem entre si por um desses objetivos,
- os que fazem isso/aquilo por meios ou para fins escusos,

induzem impasses e conflitos que se tornam elementos cada vez mais cruciais nos *processos de segurança* relativa a informação, comunicação, dados ou computação.

Também cruciais nesses processos, as confusões na percepção desses impasses e conflitos, e dos efeitos induzidos nesses impasses por iniciativas visando medidas protetivas.

1. O que é “Segurança”?

O que significa isso?

Teatro, sentimento *e* processo:

Relatório “Modelos de Confiança” (M.C.), Seção 1 e Exercício 1

1. Processo de segurança

O que é isso?

1. Processo de segurança

O que é isso?

Exemplo de aplicação da lei ou **princípio de Kerckhoffs**

1. Processo de segurança


https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html

Publications

The most dangerous code in the world: validating SSL certificates in non-browser software

Authors: *M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov*

Abstract:
SSL (Secure Sockets Layer) is the de facto standard for secure Internet communications. Security of SSL connections against an active network attacker depends on correctly validating public-key certificates presented when the connection is established. We demonstrate that SSL certificate validation is completely broken in many security-critical applications and libraries. Vulnerable software includes Amazon's EC2 Java library and all cloud clients based on it; Amazon's and PayPal's merchant SDKs responsible for transmitting payment details from e-commerce sites to payment gateways; integrated shopping carts such as osCommerce, ZenCart, Ubercart, and PrestaShop; AdMob code used by mobile websites; Chase mobile banking and several other Android apps and libraries; Java Web-services middleware - including Apache Axis, Axis 2, Codehaus XFire, and Pusher library for Android - and all applications employing this middleware. Any SSL connection from any of these programs is insecure against a man-in-the-middle attack. The root causes of these vulnerabilities are badly designed APIs of SSL implementations (such as JSSE, OpenSSL, and GnuTLS) and data-transport libraries (such as cURL) which present developers with a confusing array of settings and options. We analyze perils and pitfalls of SSL certificate validation in software based on these APIs and present our recommendations.

Exemplo de processo que se mistura (ou se confunde) com sentimento de [in]segurança no domínio das TIC (Tecnologias de Informação e Comunicação digitais)

1. Processo de segurança

"O protocolo SSL se tornou padrão de fato para comunicações seguras na Internet. Segurança em conexões SSL contra ataques de escuta ativa depende da correta validação de certificados de chaves públicas apresentados quando a conexão é estabelecida. Demonstramos que a validação de certificados X.509 é completamente quebrada em muitas aplicações de segurança crítica. Softwares vulneráveis incluem a biblioteca EC2 da Amazon Java e todos os clientes de *cloud* baseados nela; SDKs do PayPal e da Amazon para sites de comércio eletrônico que transmitem dados de pagamento para *gateways* de pagamento; carrinhos de compras integradas como osCommerce, ZenCart, Ubercart, e PrestaShop; código AdMob usado por dispositivos móveis; Chase *mobile banking* e vários outros aplicativos Android e bibliotecas; *middleware* Java Web Services - incluindo Apache Axis, Axis 2, XFire Codehaus e biblioteca Pusher para Android - e toda aplicação que emprega este middleware. Qualquer conexão SSL a partir de qualquer um destes programas é insegura contra ataques *man-in-the-middle*. A raiz das causas destas vulnerabilidades são APIs de implementa-ções SSL(p.ex. do JSSE, OpenSSL e GnuTLS) e de transporte de dados (p.ex. da cURL) mal concebidas, que apresentam aos desenvolvedores uma gama **confusa** de configurações e opções. Analisamos perigos e armadilhas na validação de certificados em programas que usam essas APIs, e damos recomendações."

https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html

1. Teatro da segurança

Pela falta de calibres aferíveis entre sentimento (plano interno) e processo (externo), vivemos o *teatro da segurança*, onde se tramam cenas entre os dois planos (psíquico e físico). Onde se tem:

- nos *enredos*: riscos, mecanismos de proteção, percepção de riscos e da utilidade desses mecanismos para agentes;
- em *cenários*: neutralidade tecnológica *e* de suas aplicações, e evolução tecnológica como sempre desejáveis e benéficas;
- no *decorrer* dos atos: sentimento relapso e atitudes ingênuas no processo agem propagando, fertilizando e nutrindo riscos

1. Teatro da segurança

Pela falta de calibres aferíveis entre sentimento (plano interno) e processo (externo), vivemos o *teatro da segurança*, onde se tra-mam cenas entre os dois planos (psíquico e físico). Onde se tem:

- nos *enredos*: riscos, mecanismos de proteção, percepção de riscos e da utilidade desses mecanismos para agentes;
- em *cenários*: neutralidade tecnológica *e* de suas aplicações, e evolução tecnológica como sempre desejáveis e benéficas;
- no *decorrer* dos atos: sentimento relapso e atitudes ingênuas no processo agem propagando, fertilizando e nutrindo riscos.

Aí se observa, no domínio das TIC, gastos crescentes com prote-ção em paralelo a perdas crescentes com incidentes de segurança
(referência: pesquise sobre *ciber security global report*)

1. Teatro da segurança “de dados”

Atores e Papéis

Quem são “Alice e Bob”?

1. Teatro da segurança “de dados”
Papéis e Situações Comunicativas

Alice e **B**ob são nomes de personagens em papéis de agentes de transmissões [intermediadas ou não] em **situações comunicativas** que envolvem *cognição* (i.e, capacidade de conhecimento)

Situação comunicativa = emissor + receptor + canal transmissivo + dados

Canal transmissivo = meio capaz de transmitir, através do tempo ou do espaço, sinais que codificam dados para algum **agente cognitivo**: **A** e/ou **B**

1. Teatro da segurança “de dados”
Situações e Cenários

Alice e **B**ob são nomes 'padrão' para *agentes principais* de transmissões intermediadas por TIC, na literatura sobre criptografia.
No correspondente teatro da segurança, TICs se encenam como bem em si mesmo, e seu cenário sociopolítico inclui as crenças:

1. De que o valor de uso das TIC, em geral, compensa ou supera os riscos induzidos nestes usos;
2. De que o mercado deve regular o uso das TIC ... exceto quando algum interesse concentrador (de capital/poder) é atingido;
3. De que os efeitos indiretos de 1. e 2. nos perfis de riscos dos envolvidos se racionalizam.

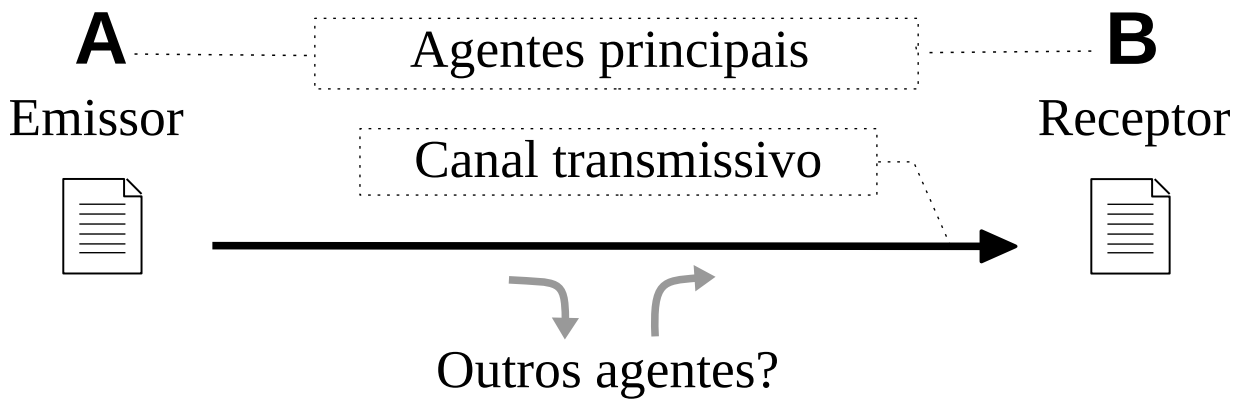
1. Teatro da segurança “de dados”
Tecnociência como ideologia

Alice e **B**ob são nomes 'padrão' para *agentes principais* de transmissões intermediadas por TIC, na literatura sobre criptografia.
No correspondente teatro da segurança, TICs se encenam como bem em si mesmo, e seu cenário sociopolítico inclui as crenças:

1. De que o valor de uso das TIC, em geral, compensa ou supera os riscos induzidos nestes usos; (ex: Aegis vs Khibiny)
2. De que o mercado deve regular o uso das TIC ... exceto quando algum interesse concentrador (de capital/poder) é atingido;
3. De que os efeitos indiretos de 1 e 2 (ex: *social cooling*, 737max, nos perfis de riscos dos envolvidos se racionalizam. AI-5d)

Onde qualquer outra abordagem é desprezada como 'ideológica'
(ver Rubens Casara, 2017: "Estado pós-democrático")

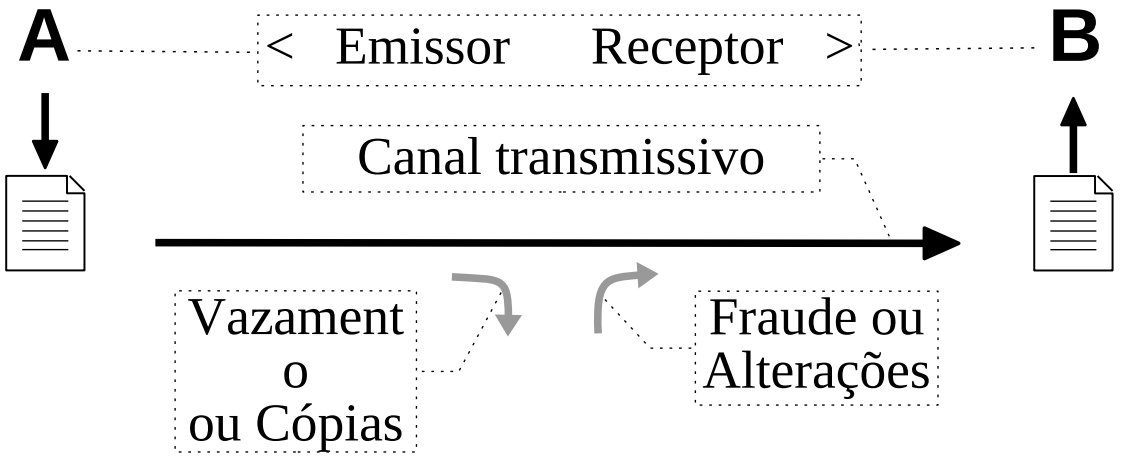
1. Teatro da segurança “de dados”
Planos de enredo: Físico e Psíquico



Ação que melhor corresponde ao substantivo “segurança”: a do verbo *proteger*. No processo (plano físico), um verbo *bitransitivo*:
Protege-se *alguém* (ou algo), *de* (ou contra) *algo*.

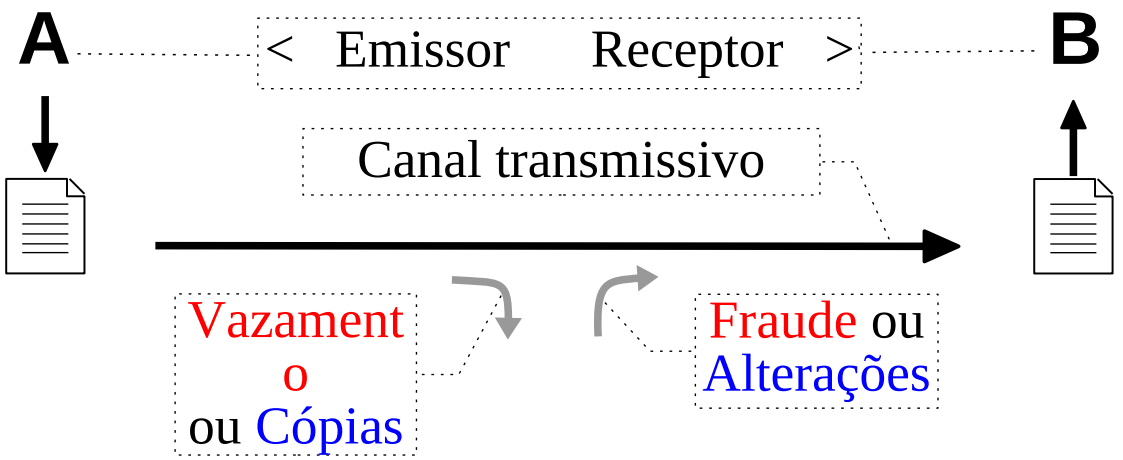
Segurança: No processo – *de que*[*m*], contra *o quê*? Na psique – risco aceitável?

2. O que é Comunicação
no Teatro da Segurança “de dados”?



Que tipo de ação significa “proteger dados”?

2. O que é Comunicação
no Teatro da Segurança “de dados”?

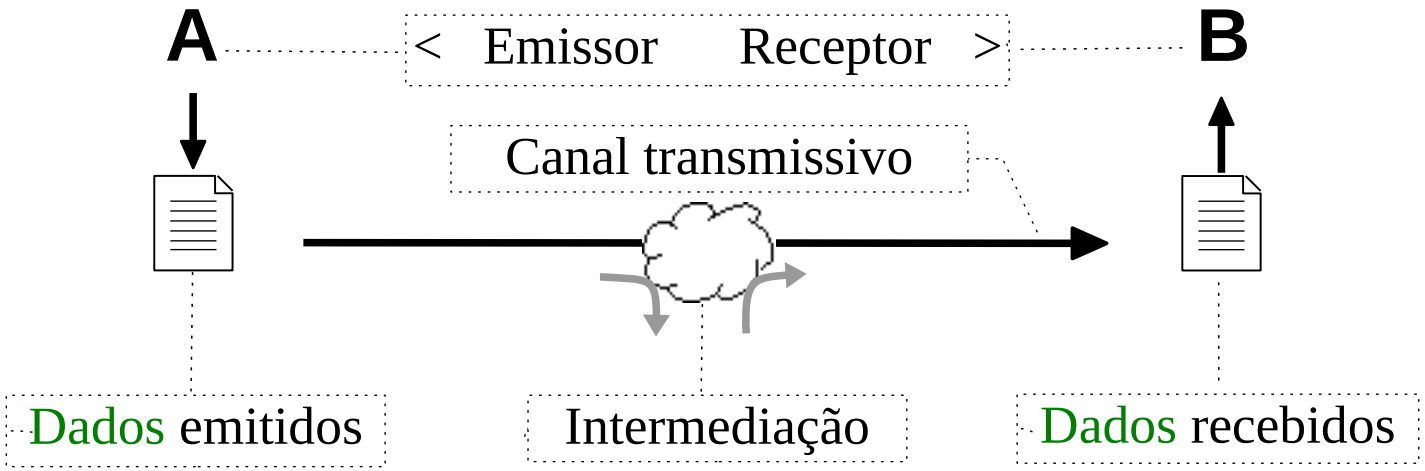


Que tipo de ação significa “proteger dados”?

No processo: Evitar *ou* permitir certas ações ao longo do canal transmissivo, em *uma* dada situação comunicativa, conforme *um* contexto de referência para proteção.
Referência: a *interesse*(*s*) do agente **A**, do **B**, do dono do canal, ou combinações.

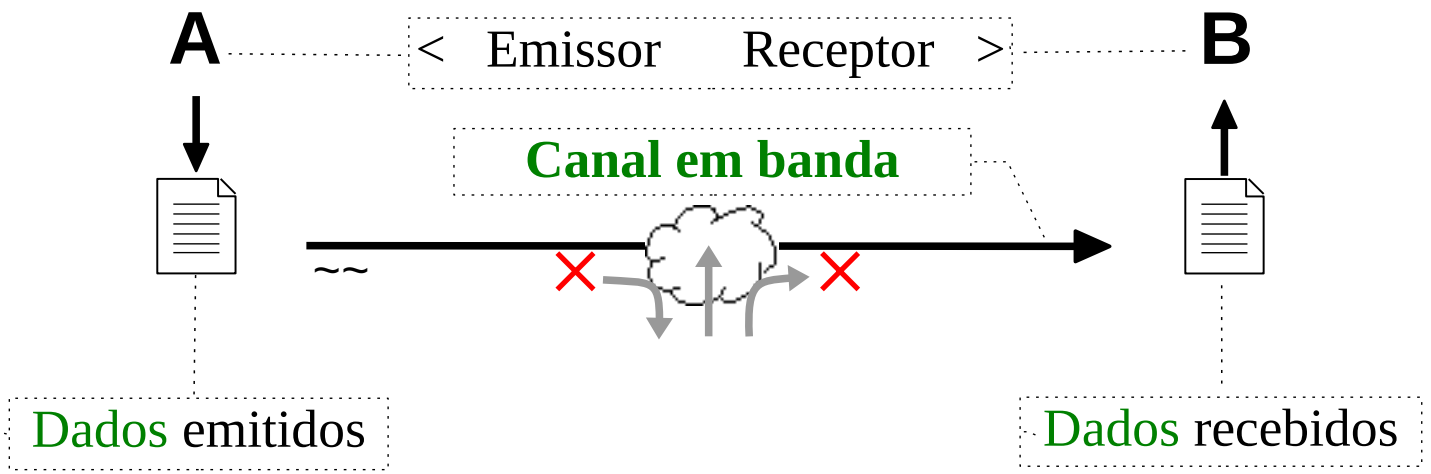
Na psique: induzir sentimento de que tais interesses, na situação comunicativa e contexto em foco, estão protegidos.

2. O que é Comunicação
no Teatro da Segurança “de dados”?



Para que serve a Criptografia nesse teatro?

2. O que é Comunicação
no Teatro da Segurança “de dados”?



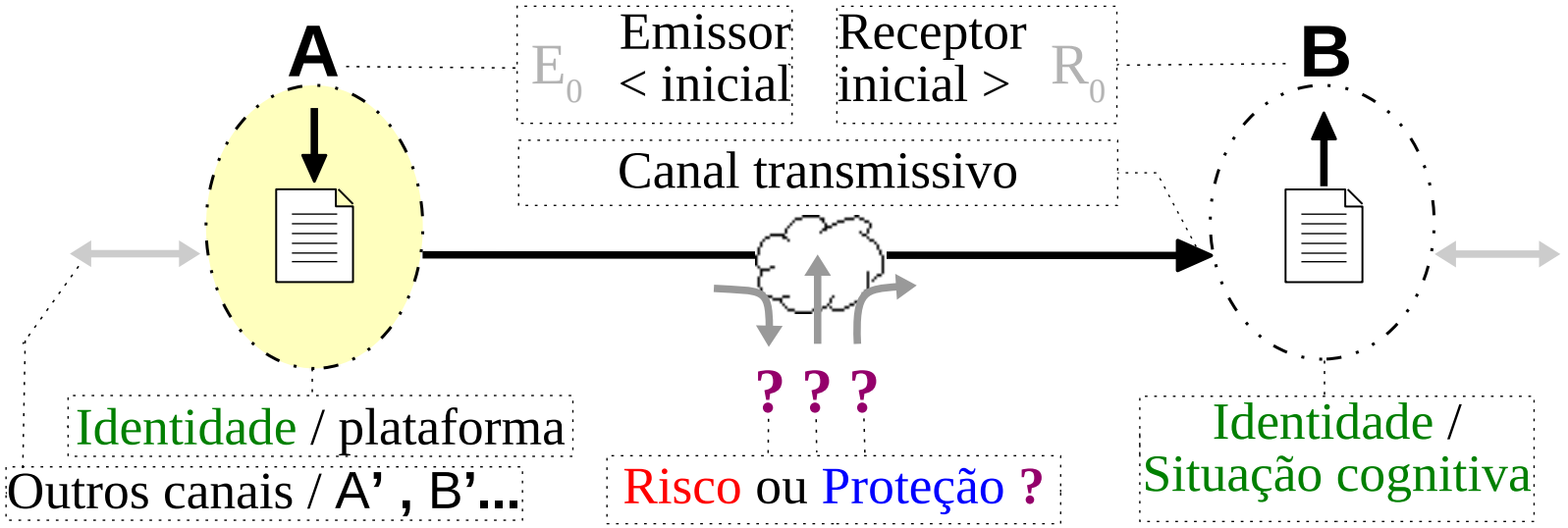
Para que serve a Criptografia nesse teatro?

No processo: para proteger *sigilo e/ou integridade* daquilo que dados significam, *e/ou acesso* a tais dados, *durante a transmissão* dos mesmos através de um canal vulnerável.

Se esse canal for digital ou virtual, costuma ser chamado de ‘**Canal em Banda**’

2. O que é Comunicação
no Teatro da Segurança "de dados"?

Shakespeare: "*All the world is a stage. And all the men and women merely players; They have their exits and their entrances…*"

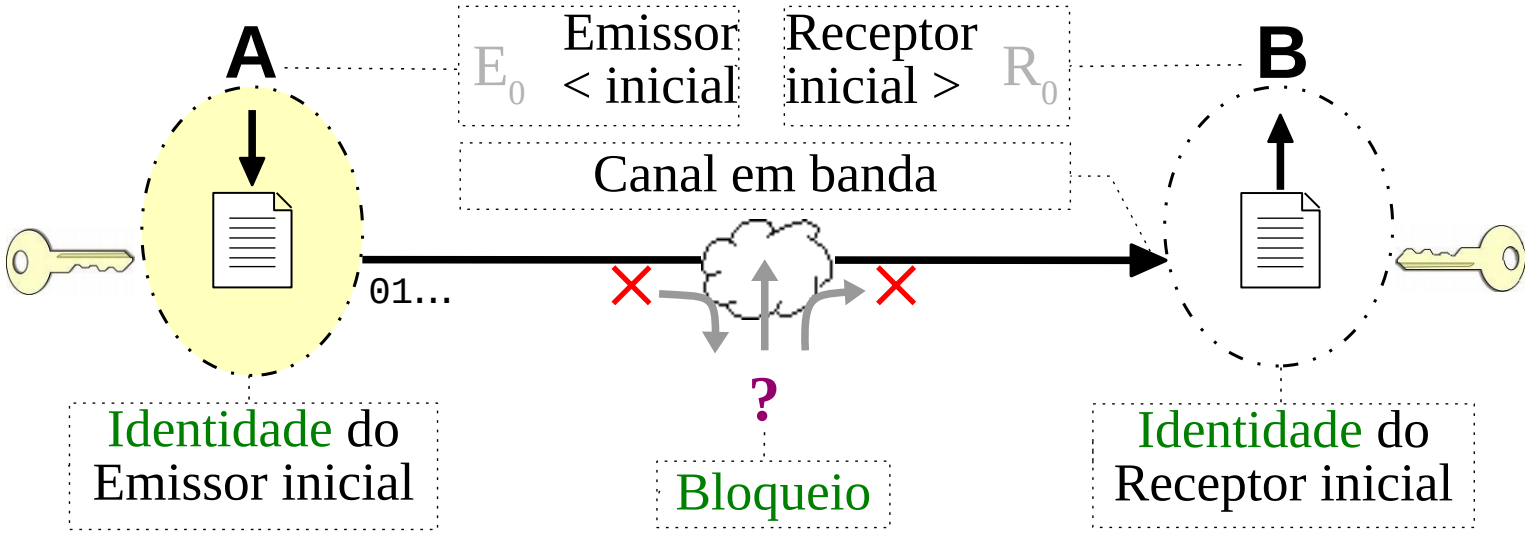


Enredo básico nesse *Teatro Humano*: Comunicação (a própria) – Para que/quem transmitir ou receber sinais/dados, quais, e como?

Teatro Humano [**TH**]: Para indivíduos, a questão de como atuar em situações comunicativas está psiquicamente inserida no drama do sentido de suas vidas (alteridade). Seus *interesses* {} tendem a buscar certas proteções para o que os dados possam significar.

2. O que é Comunicação
no Teatro da Segurança “de dados”?

Shakespeare: “*All the world is a stage. And all the men and women merely players; They have their exits and their entrances…*”



Como o uso da Criptografia presume identificação, sob o princípio de Kerckhoffs?

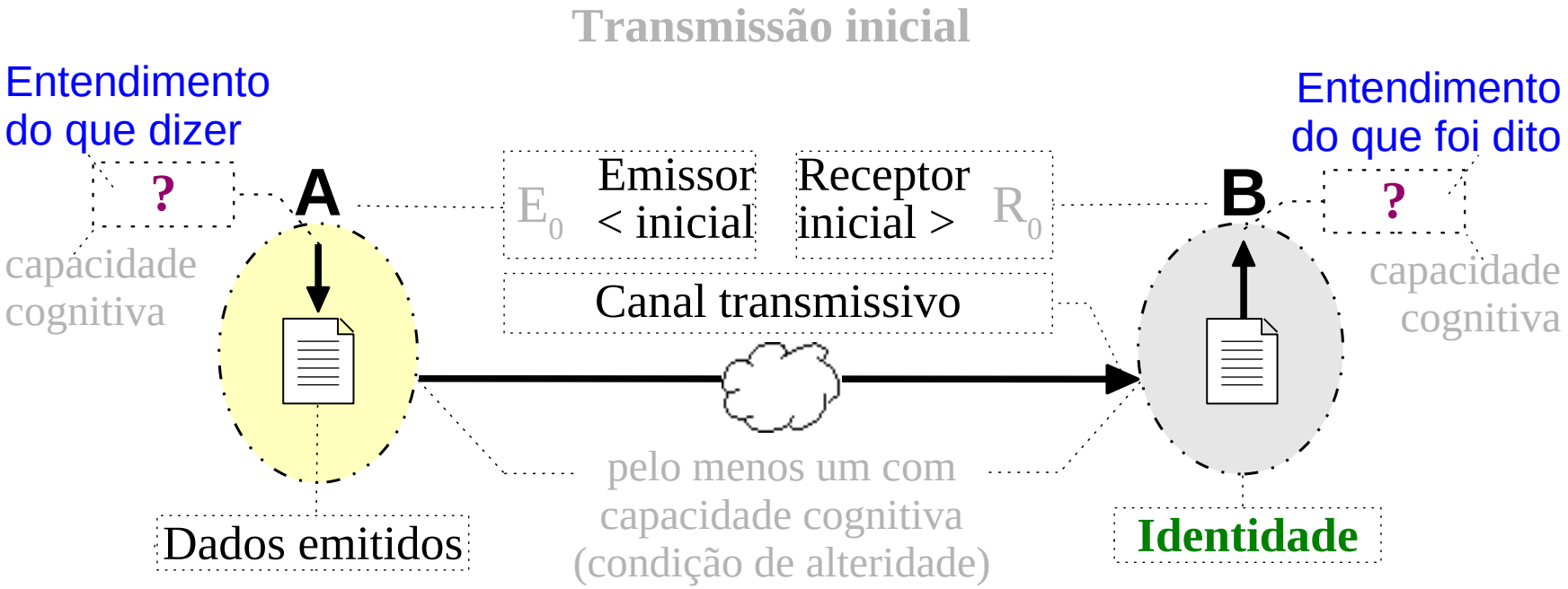
Subtrama em enredos do **TH**: Quem e para quem enviar ou distribuir mecanismos ou recursos criptográficos (chaves, etc), quais, para que, e como? [***Key Distribution Problem***]

2. O que é **Criptografia**?

Arte[1], engenharia[2] e ciência[3] de *escrita oculta*

- Criptografia *não* protege comunicação, **dado** ou informação *em si*
  Dados são meros símbolos, codificados em sinais quantificáveis, capazes de representar informação em contextos (Valdemar Setzer)
- Símbolos *não* pegam fogo nem vão para a cadeia, não quebram nem morrem; *o que* eles informam, ou *a quem* significam*, talvez.
- O que Criptografia pode proteger são certos *valores* que os dados significam, ante algum *interesse*, pelo que informam *em contextos*
- Esses **valores protegíveis** são os que podem ser preservados por garantias de sigilo, *e/ou* de integridade, *e/ou* de acesso controlado.
- Garantias *relativas*, porque mecanismos criptográficos funcionam com base em dois fundamentos, dos quais ao menos um é relativo
  - Controle de custos de [2]codificações/decodificações (para uso);
  - *Premissas de confiança* ([1]condições para tal uso ser [3]eficaz).

3. Como se produzem significados
em situações comunicativas

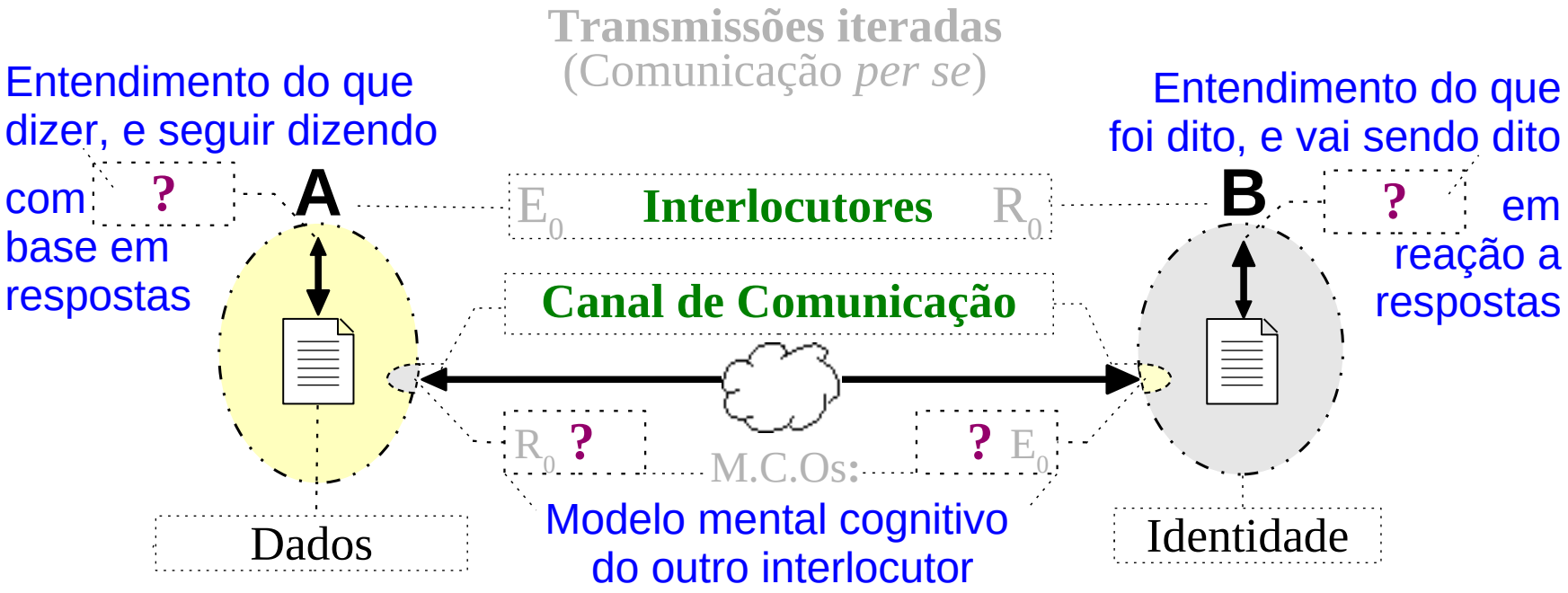


* **TH** (continuação): Significar *para quem*? O que é "quem", "identidade", "significado"?

Identidade (Muniz Sodré, 1994)**:** mera projeção {◯}, que fixa características – que são fluidas e mutáveis – em um ente ou de um indivíduo.

Identificação é portanto qualquer (sub)processo que fixa tais projeções. E "quem" é mero pronome, usado na narrativa do processo para se referir a algum *agente cognitivo*

3. Como se produzem significados
em situações comunicativas



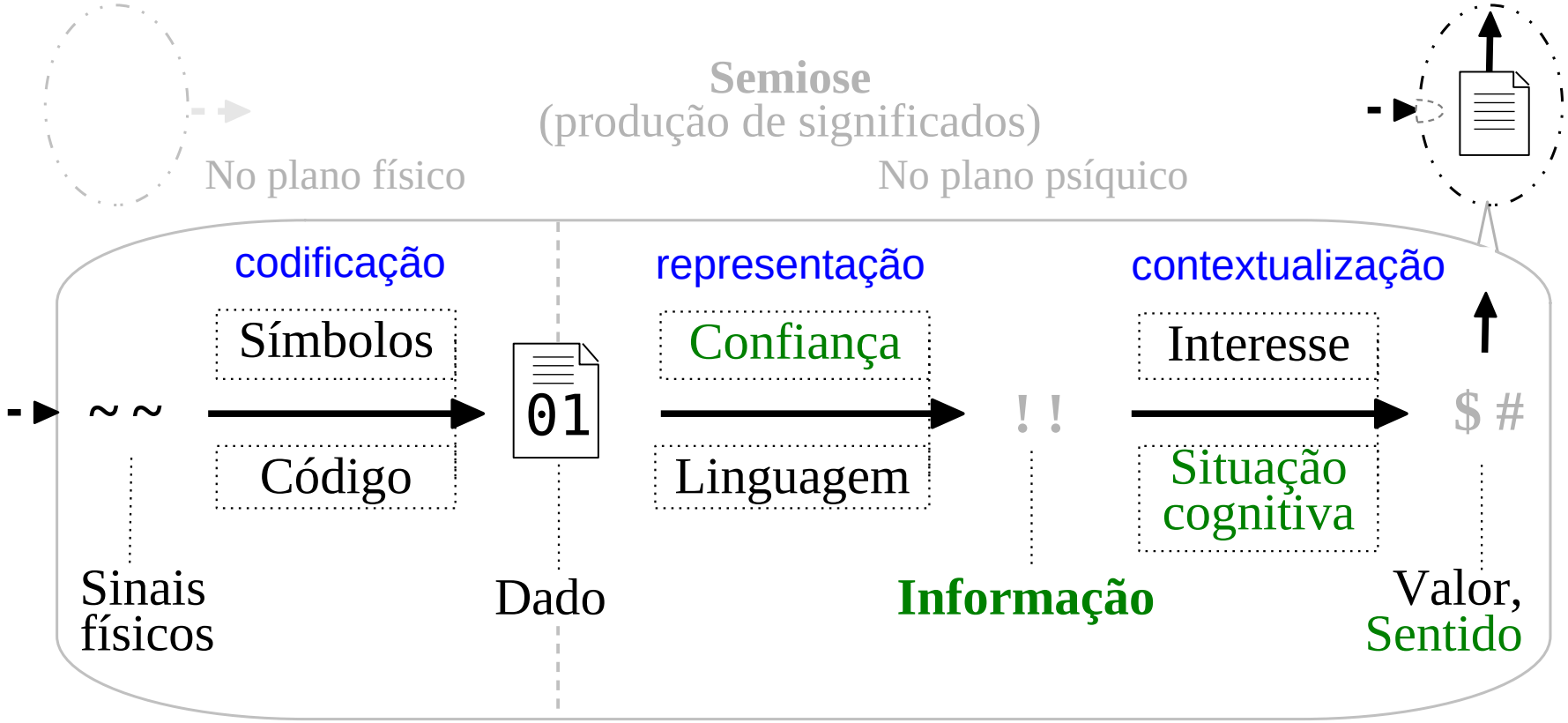
Canal de Comunicação = canal transmissivo *bidirecional* + modelos cognitivos do outro

Significado: O que se produz cognitivamente em agentes principais, com estes alternando papéis – mesmo que simulados – de emissor e receptor.

Quando emissor e receptor se alternam num canal de comunicação, para se destacar tal alternância (mesmo simulada) esses agentes cognitivos são chamados '**Interlocutores**'

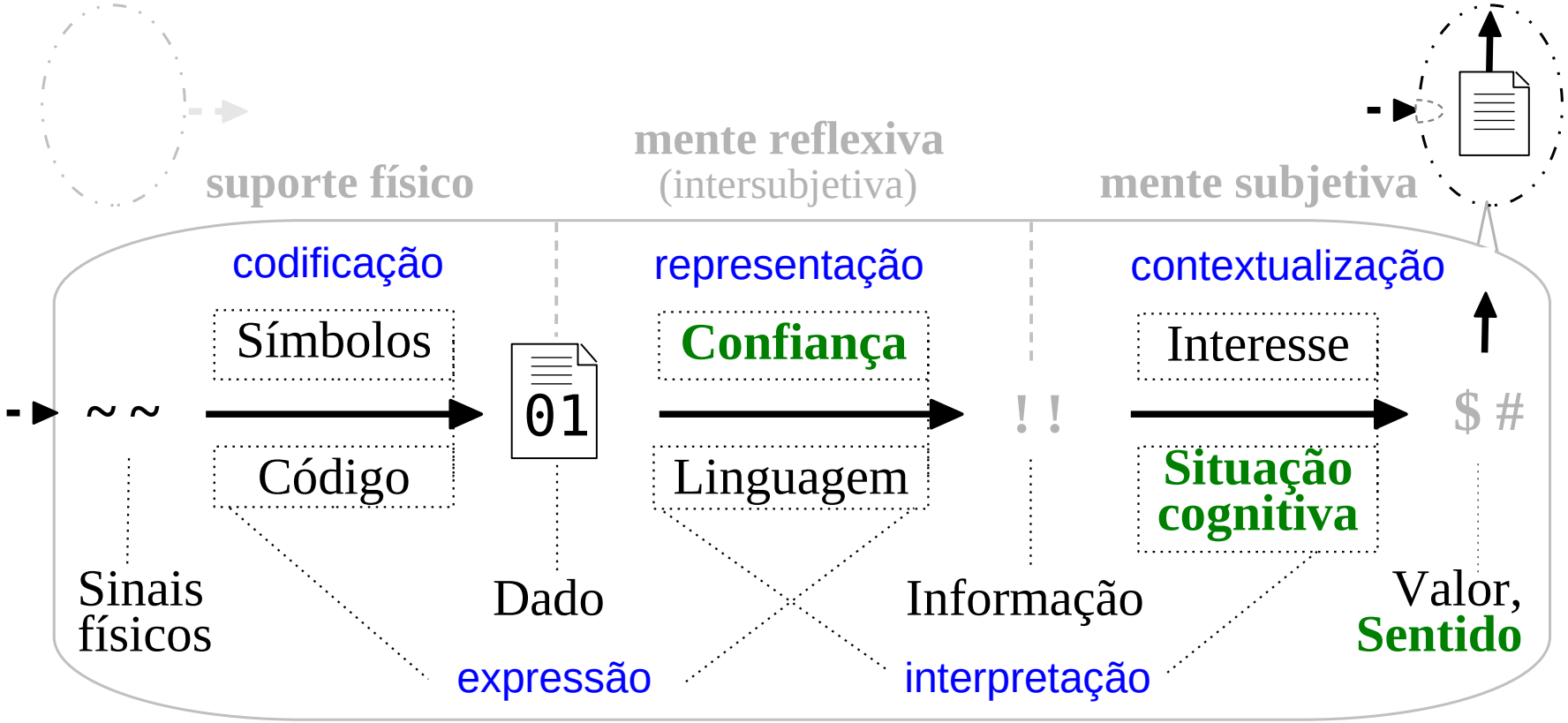
3. Como se produzem significados

Etapas do processo



Informação (Shannon, 1948): Aquilo que é *transferido* de uma fonte emissora para um destino através de um *canal*, medível em termos de probabilidade do que *não é antecipável* em relação ao que pode *ser esperado e entendido** [do contexto] pelo receptor. *(envolve cognição)

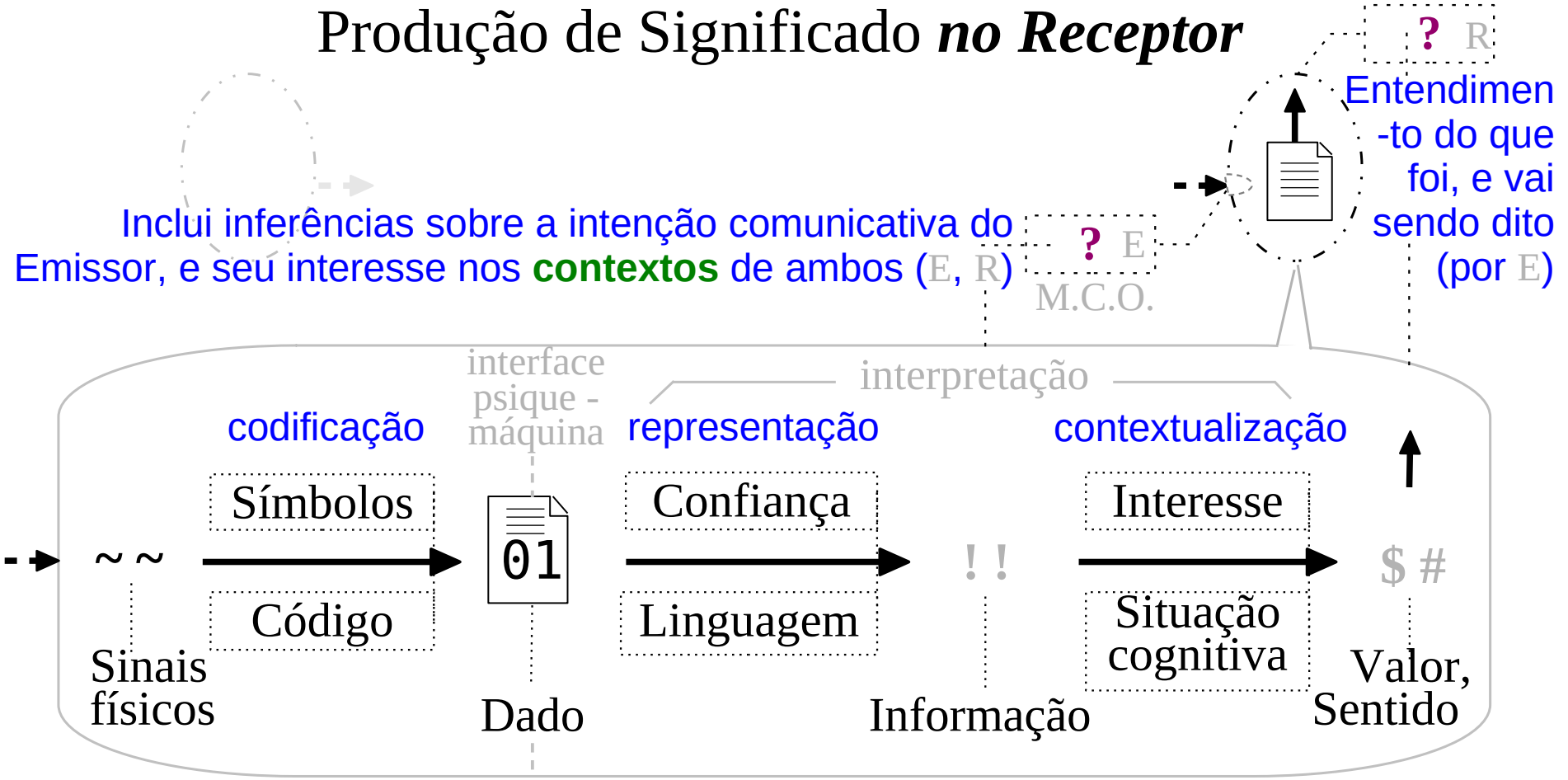
3. Como se produzem significados:
Semiose na comunicação humana



Confiança (Ed Gerk, 1997)**:** Aquilo que é *essencial** para um canal de comunicação e que *não pode ser transferido* da fonte ao destino *através deste canal.* [**Situação cognitiva** é aquilo que se crê já sabido]

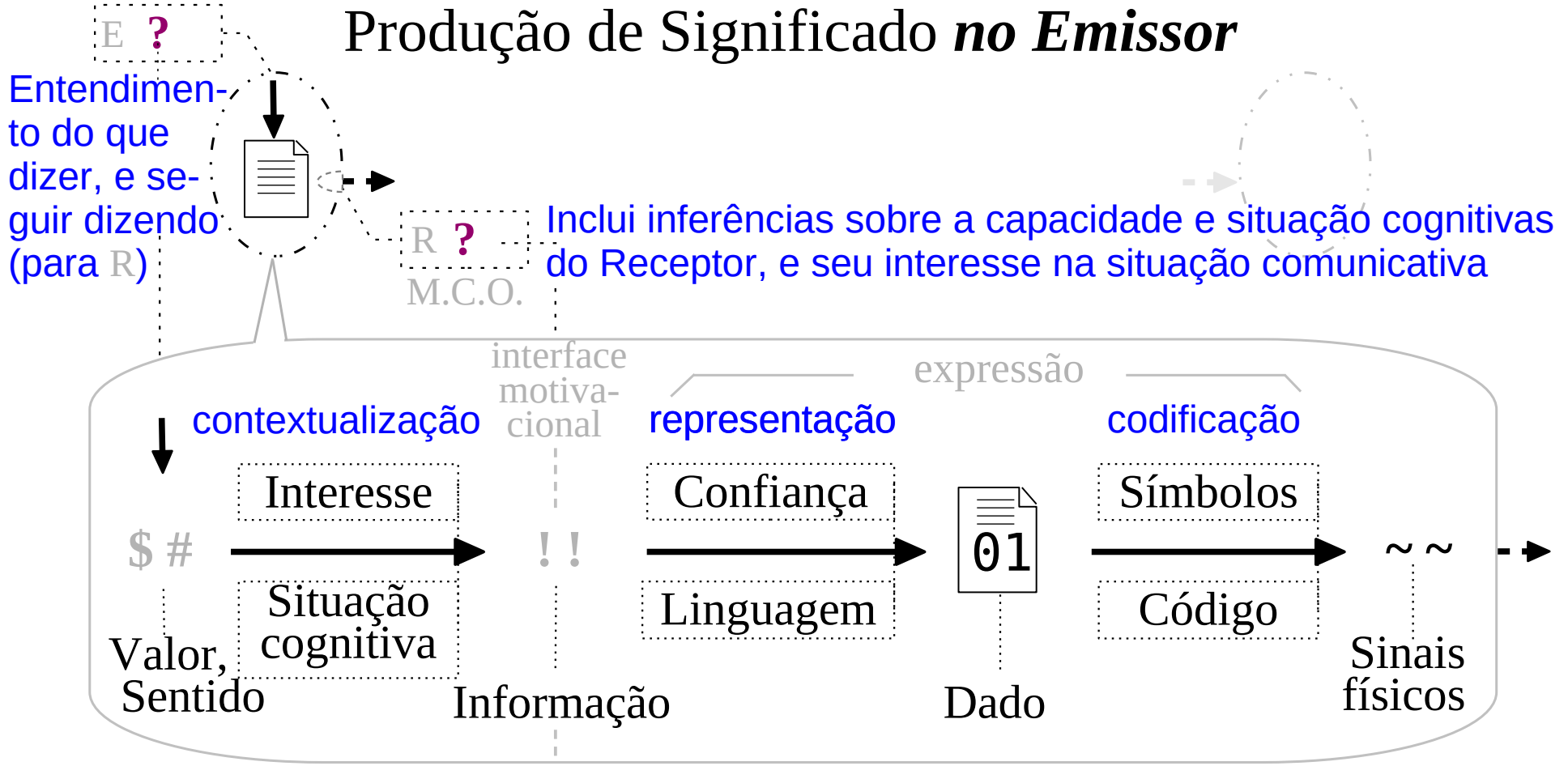
* para informação ter valor ou fazer **sentido** (i.e, dar significado *coerente*)

3. Como se produzem significados
Fases direcionadas da semiose



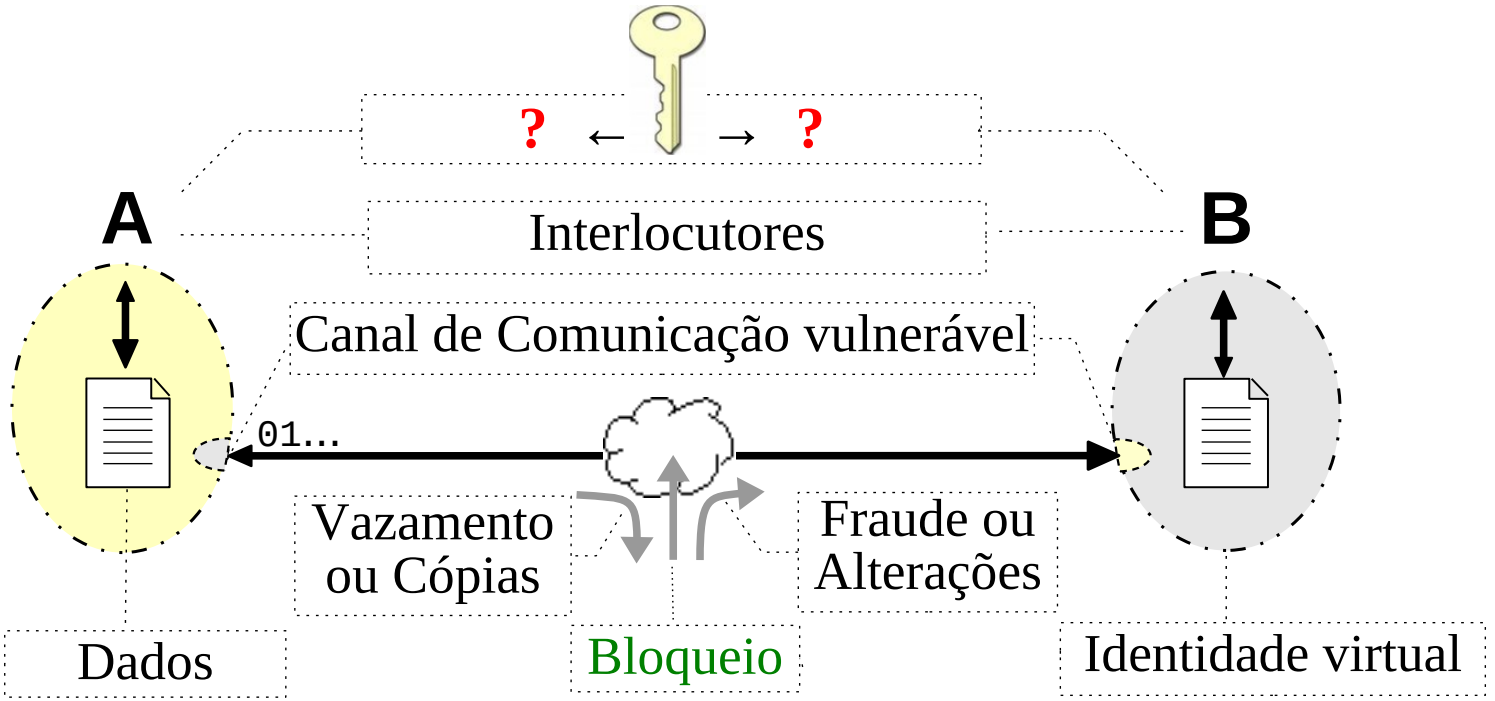
Contexto: estado de conhecimento 'filtrado em confiança'* para decidir *se, e como*, engajar o outro interlocutor, e atualizar tal estado em função das iterações decorrentes

3. Como se produzem significados
Fases direcionadas da semiose



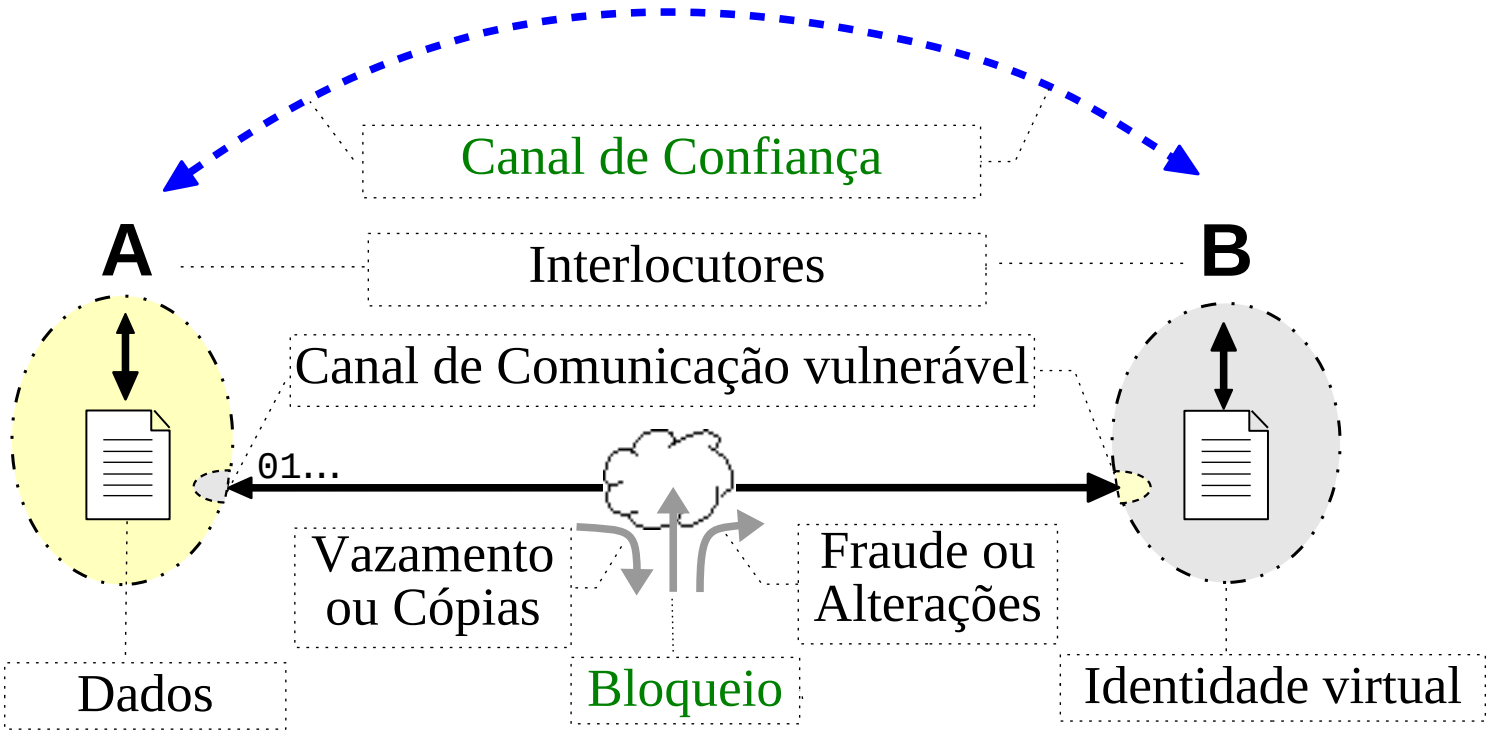
* Confiança **Direcionada:** atua como filtro (*in*) – no papel de emissor, para expressão; e no de receptor, para interpretação, fundados em *suposto* interesse(s) do outro interlocutor

4. Processo de segurança
Em contextos virtuais



Como podem ser protegidos interesses *relativos a uma situação comunicativa em foco*, durante transmissões digitalmente intermediadas, através de um canal em banda vulnerável?

4. Processo de segurança
Em contextos virtuais

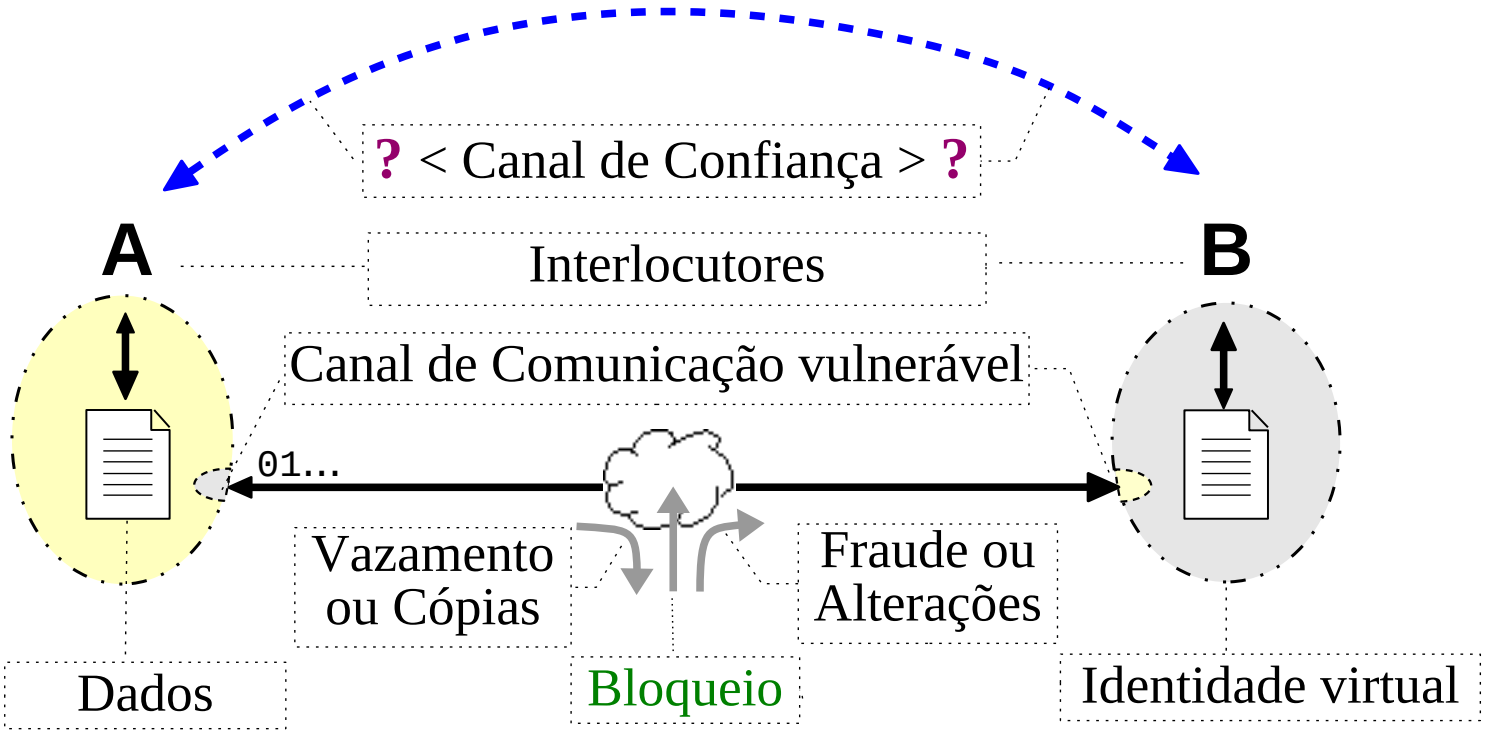


Com *prévio* transporte *confiável* de recursos que habilitam o uso *eficaz* de mecanismo(s) de proteção em banda (‘*key distribution*’) *adequado*(*s*) [se houver] à proteção do(s) interesse(s) em foco.

4. Segurança computacional
Processo

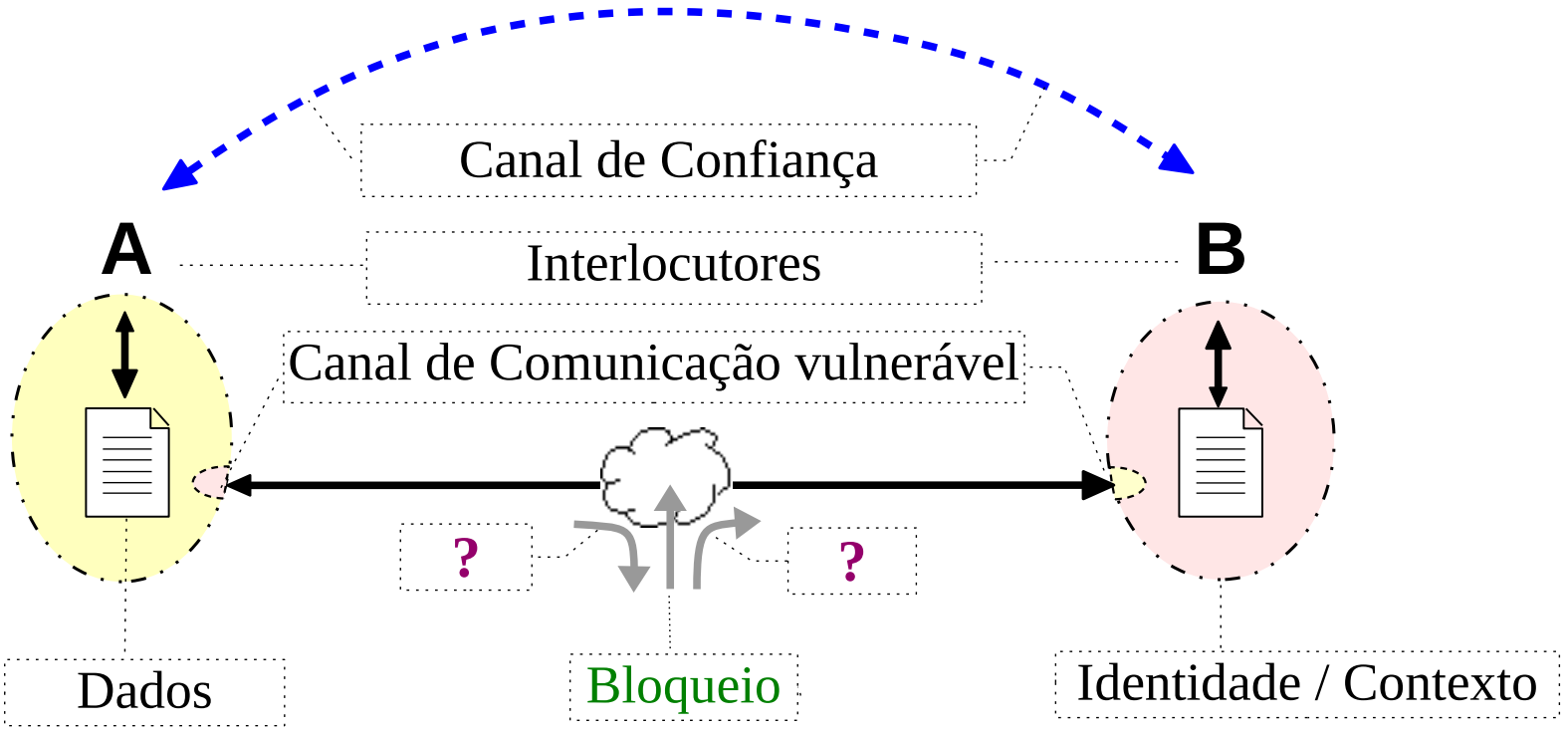
- O uso *eficaz* de *qualquer* tal mecanismo requer certas condições para produção, transporte, armazenagem e operação de recursos, material *necessário* à execução do(s) mecanismo(s) escolhido(s).
- Na informática, esse material nescessário é formado, geralmente, por seqüências binárias em codificações próprias: senhas, chaves criptográficas, *nounces*, algoritmos em formato executável, etc.
- Já o uso *adequado*, requer escolhas próprias à proteção almejada. As condições e requisitos para uso eficaz do(s) mecanismo(s) escolhido(s) são chamadas **Premissas de Confiança** [nessa escolha]
- **Canal de Confiança** designa canal *fora-de-banda* (fora do tempo e/ou do espaço do c. em banda) que seja confiável para as premissas de confiança *referentes ao transporte* de material necessário ao(s) mecanismo(s) escolhido(s) para operar(em) em banda.

4. Segurança computacional
Processo



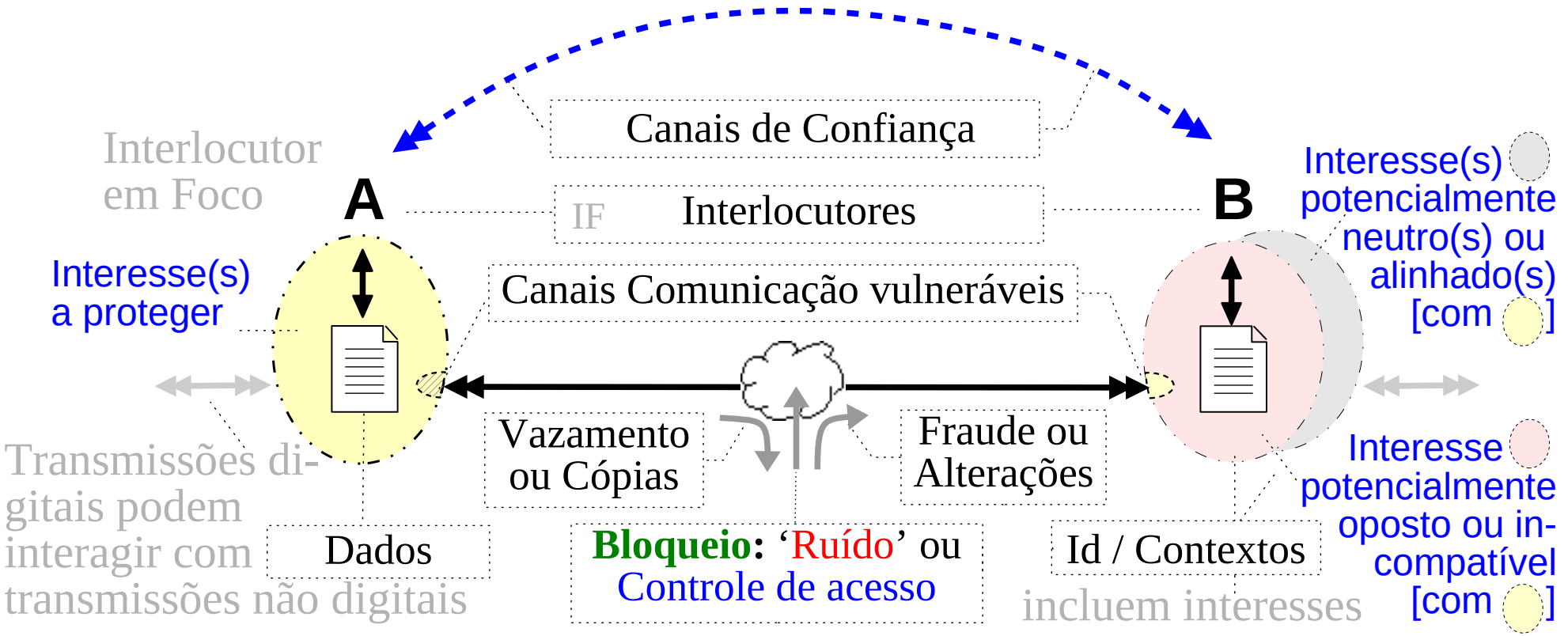
Como escolher mecanismos de proteção em banda adequados ao(s) interesse(s) de um (ou mais) agente(s) ou interlocutor(es) para situações comunicativas e cognitivas específicas?

4. Segurança computacional
Planejamento e ...



Com uma **politica de segurança.** Há contextos onde, *dos mesmos dados e ao mesmo tempo*, a um interlocutor interessa o sigilo enquanto ao outro, integridade apenas (transparência), onde nenhum deles é mais 'dono' dos dados, e uma coisa protege *contra* a outra.

4. Segurança computacional
… Execução



<u>Política de segurança</u> começa com: Escolhas adequadas *para quem*, *onde*, *quando*? Aí começa o jogo do poder acerca da segurança "de dados" – i.e, *informacional* – em contextos virtuais.

4. Segurança computacional
Eficácia

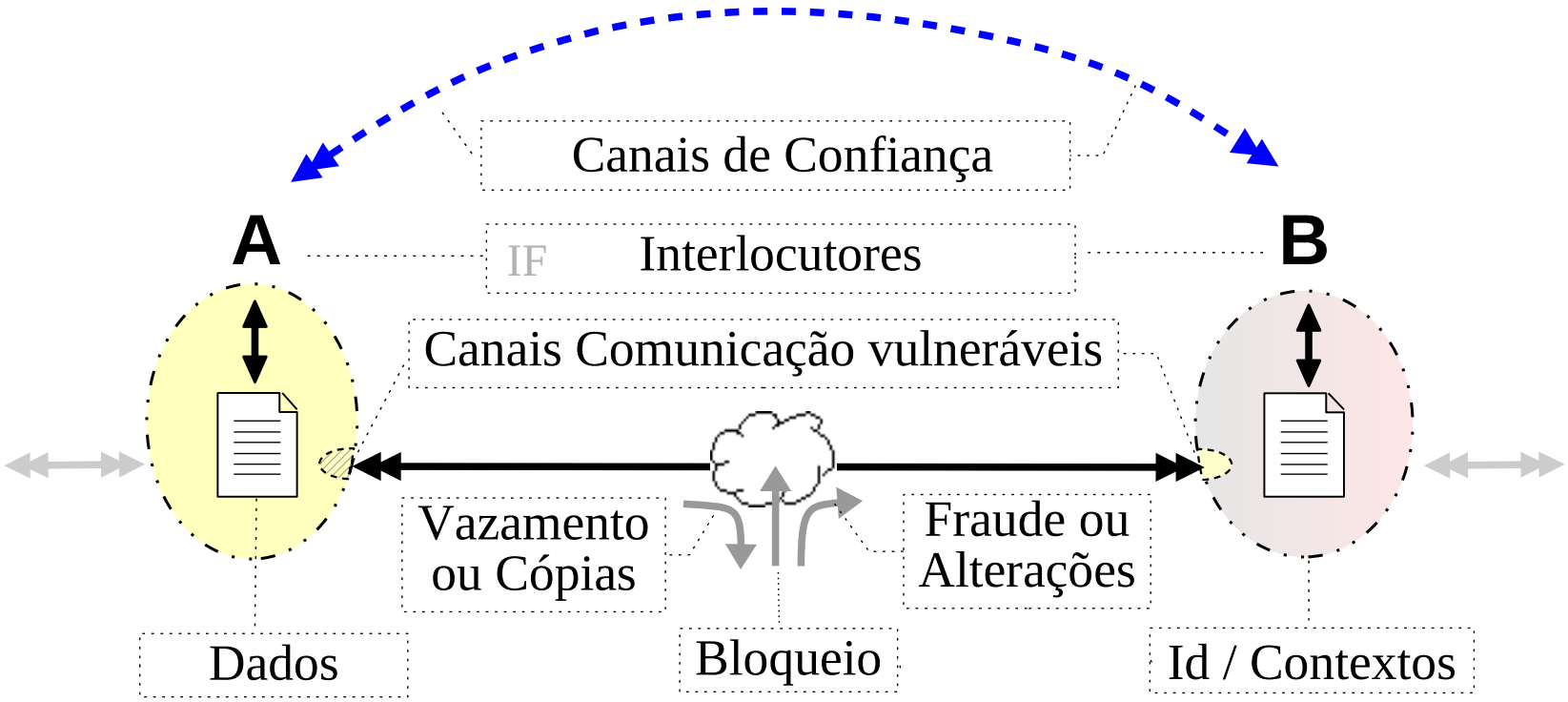
- Conforme quem (**A** e/ou **B**, etc) contempla proteger em banda *o que*, *contra o que*, e *como*, presume-se haver, *antes do uso do*(*s*) *mecanismo*(*s*) *escolhido*(*s*) [para a proteção], alguma garantia: para quem gera ou remete *material que habilita* tal(is) mecanismo(s), sobre a identidade do destinatário, e/ou vice-versa, e sobre a origem, a integridade, e em certos casos o sigilo, desse material.

- Exemplo: Se a escolha incluir cifra assimétrica, as Premissas de Confiança não exigem sigilo no Canal de Confiança *para material dessa cifra* (chave pública, executáveis), *mas* exigem integridade

- **Questões básicas**, relacionadas ao *Key Distribution Problem*:

  a) Pode a Criptografia ser eficaz *sem* Canais de Confiança?
  b) Pode a Segurança na informática, ou a relativa a informação?
  c) Se não, como seu uso é demandado nas situações a abordar?

4. Segurança informacional
Eficácia



Hipótese de Trabalho [Relatório M.C., 2008]**:** Questões **a)** e **b):**

Não **–** Qualquer procedimento ou mecanismo objetivando alguma forma de segurança informacional ou na informática demanda algum Canal de Confiança para habilitar seu uso eficaz. [**HT**]

4. Segurança informacional
Eficácia

- Para responder, validando a Hipótese de Trabalho, à questão **c)**

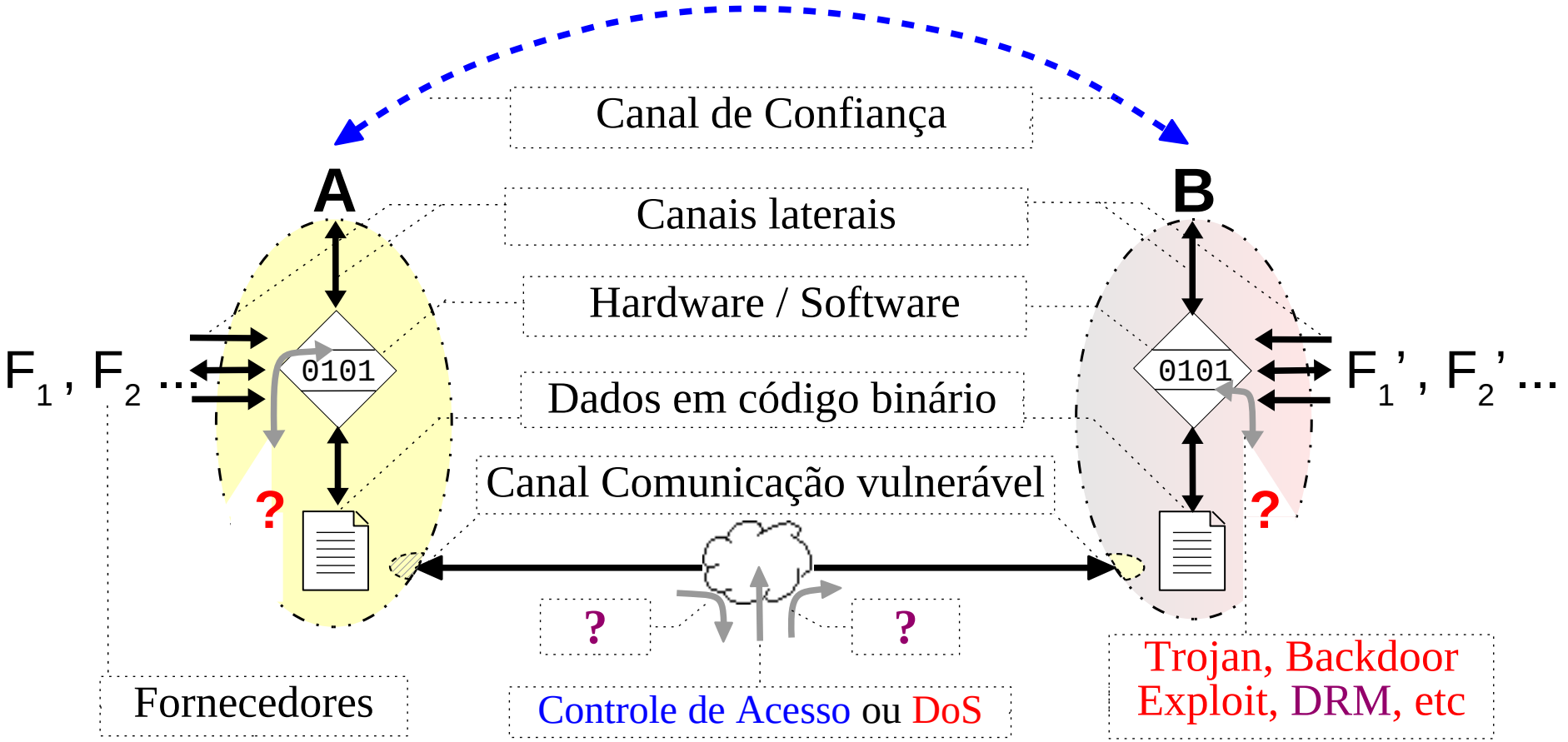
> *Como um mecanismo ou procedimento de segurança informacional demanda um Canal de Confiança?*

analisamo-la pelo referencial de interesses de quem confia, em algo ou alguém sobre algum assunto, em potencial conflito com outros interesses que induzem riscos relevantes, *relativos* às situações [comunicativa e cognitivas] e contextos [de E_0 e R_0] em foco;

Sejam esses interesses representados no processo de segurança por pessoas, instituições, programas executáveis ou máquinas.

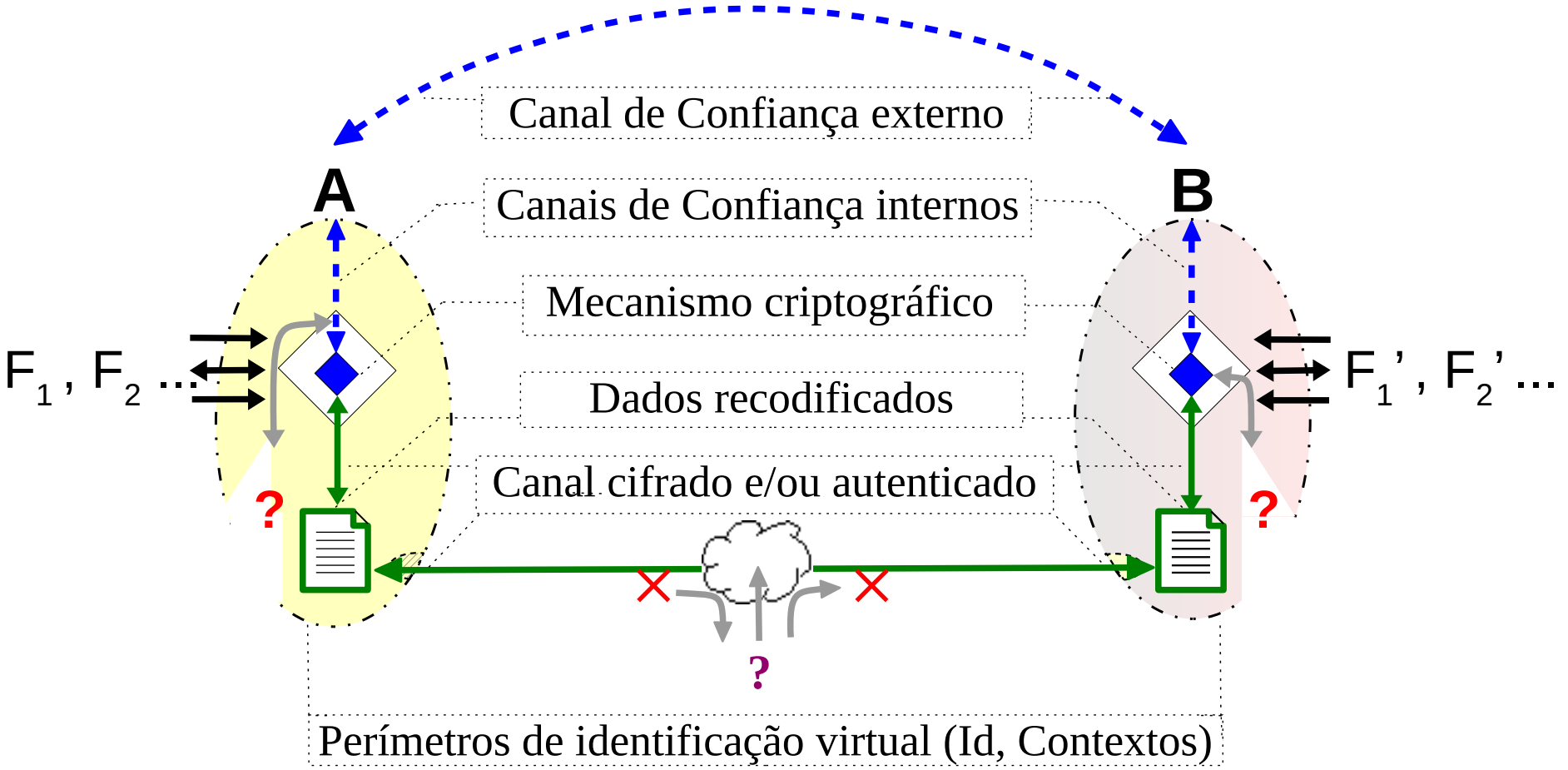
- Seguindo Garfinkel & Spafford [M.C.26], há que se considerar os interesses de *fornecedores das tecnologias* intermediadoras, e os que podem se fazer representar na operacionalização destas, como pertinentes à análise de riscos em situações intermediadas.

4. Segurança na informática
Eficácia relativa



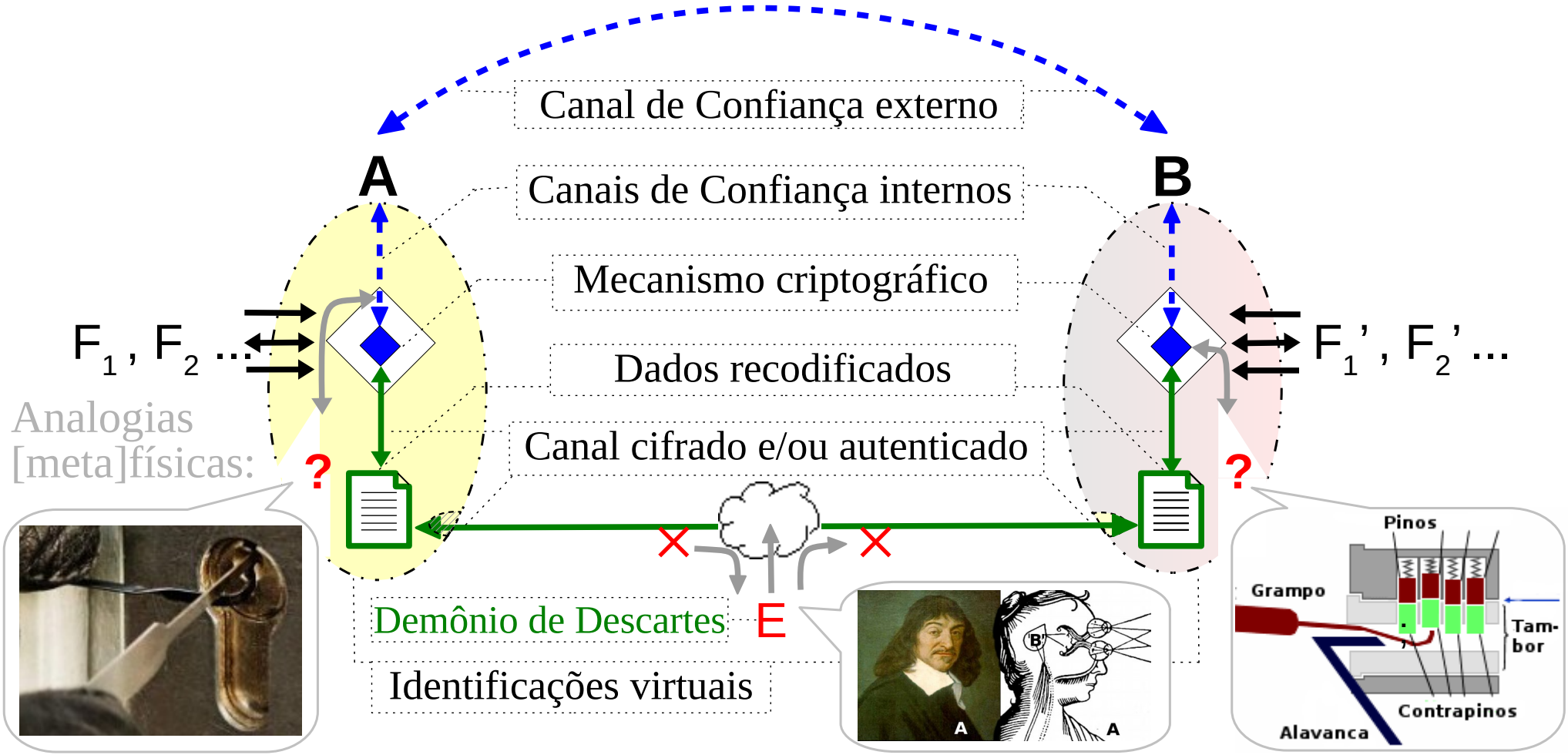
O uso adequado de TIC numa situação comunicativa protegida supõe ambientes computacionais (inclui canais laterais) sadios

4. Segurança na informática
Eficácia relativa



Ataques via canal lateral ou sobre Canal de Confiança – inclusive internos – tornam ineficaz *qualquer* mecanismo criptográfico

4. Segurança na informática
Eficácia relativa



Ataques via canal lateral ou sobre Canal de Confiança – inclusive internos – tornam ineficaz *qualquer* mecanismo criptográfico