

Segurança da Informação

Infra-estrutura de Chaves Públicas ICP-Brasil

O Problema da Autenticação

- Fácil: estabelecer um canal de comunicação sigilosa entre duas entidades (por exemplo, Diffie-Hellman).
- Difícil: verificar a identidade do interlocutor.
- Apresentação de evidência de identidade pode ser feita sobre um canal potencialmente inseguro?

Autoridade Certificadora (AC)

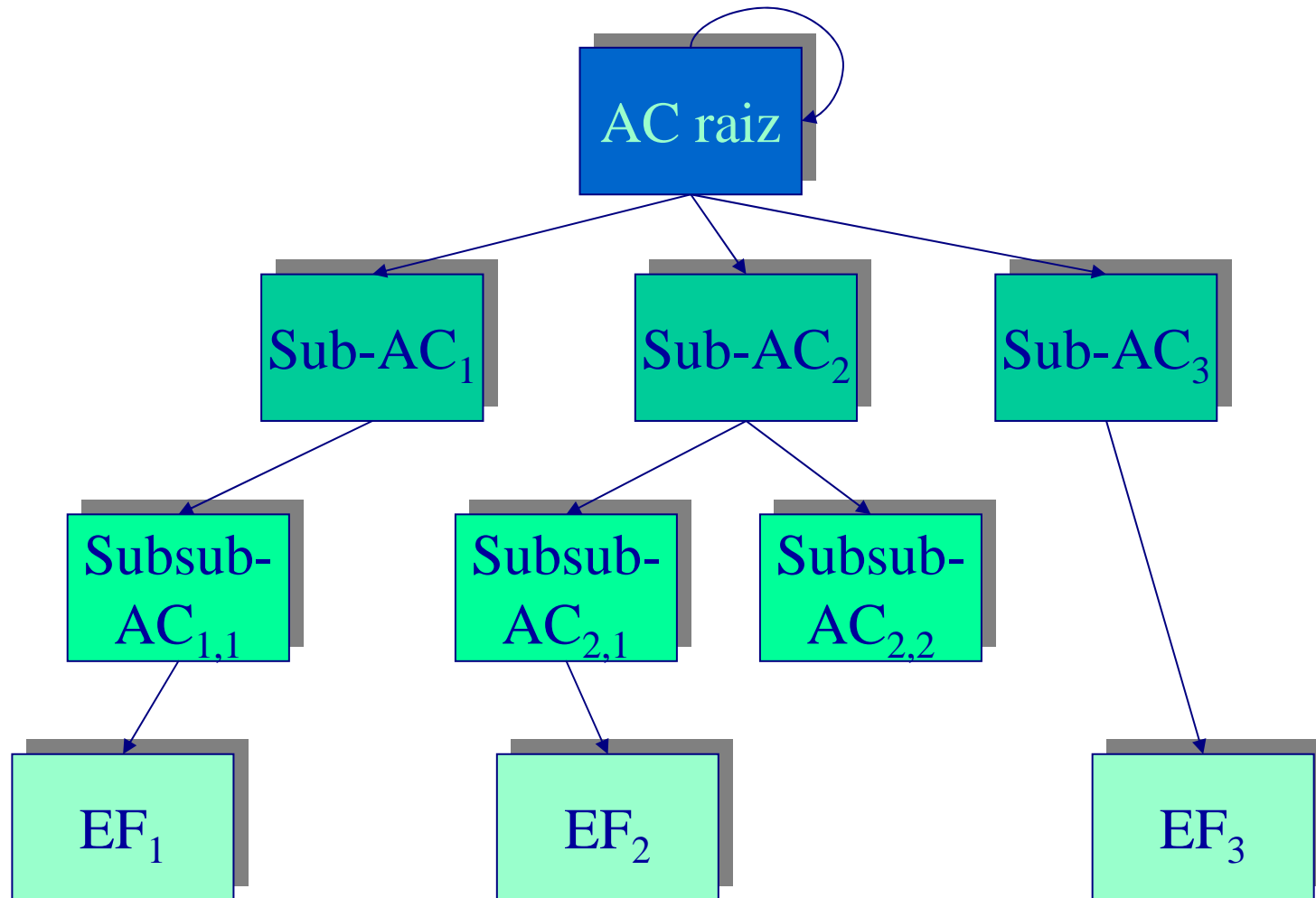
- Entidade jurídica ("tabelião eletrônico").
- Centraliza o papel de atestar a identidade de entidades finais e/ou de outras AC's.
- Certificado digital: documento eletrônico de identidade, contendo informações sobre o proprietário (incluindo sua chave pública) e sobre a autoridade certificadora emissora (incluindo uma assinatura digital).



Hierarquia de Certificação

- AC's dedicadas a vários fins.
- Proteção das chaves mais críticas.
- Caminho de certificação (da EF até a AC raiz da hierarquia).

Hierarquia de Certificação



Processo de certificação

- A entidade interessada, ou entidade final (EF), apresenta sua chave pública e demonstra sua identidade, por meios legais extra-criptográficos, para uma entidade central juridicamente confiável, a autoridade certificadora (AC).
- A EF recebe diretamente da AC um certificado de identidade individual e o certificado da própria AC.

Resultados

- O problema da demonstração de identidade fica reduzido a uma única interação, por canal fisicamente seguro, com uma entidade sujeita a vínculos jurídicos.
- Na mesma interação, obtém-se um meio íntegro de verificar a identidade de quaisquer outras entidades certificadas pela mesma AC, a saber, o certificado dessa AC.

Autoridade Registradora (AR)

- Delegada por uma AC com a responsabilidade de identificar entidades finais.
- Serviço descentralizado (por exemplo, distribuído geograficamente).

Hipótese Fundamental

- O certificado da AC raiz é obtido através de um canal confiável e legítimo por todas as partes interessadas.
- Obviamente, a segurança de toda a hierarquia de certificação depende desta hipótese.

Prova de Identidade

- Qualquer entidade que queira certificar-se precisa demonstrar sua identidade perante a AC (ou AR).
- Os critérios de demonstração de identidade são de natureza *jurídica* (dependem da legislação e das políticas da AC).

Conteúdo de um Certificado

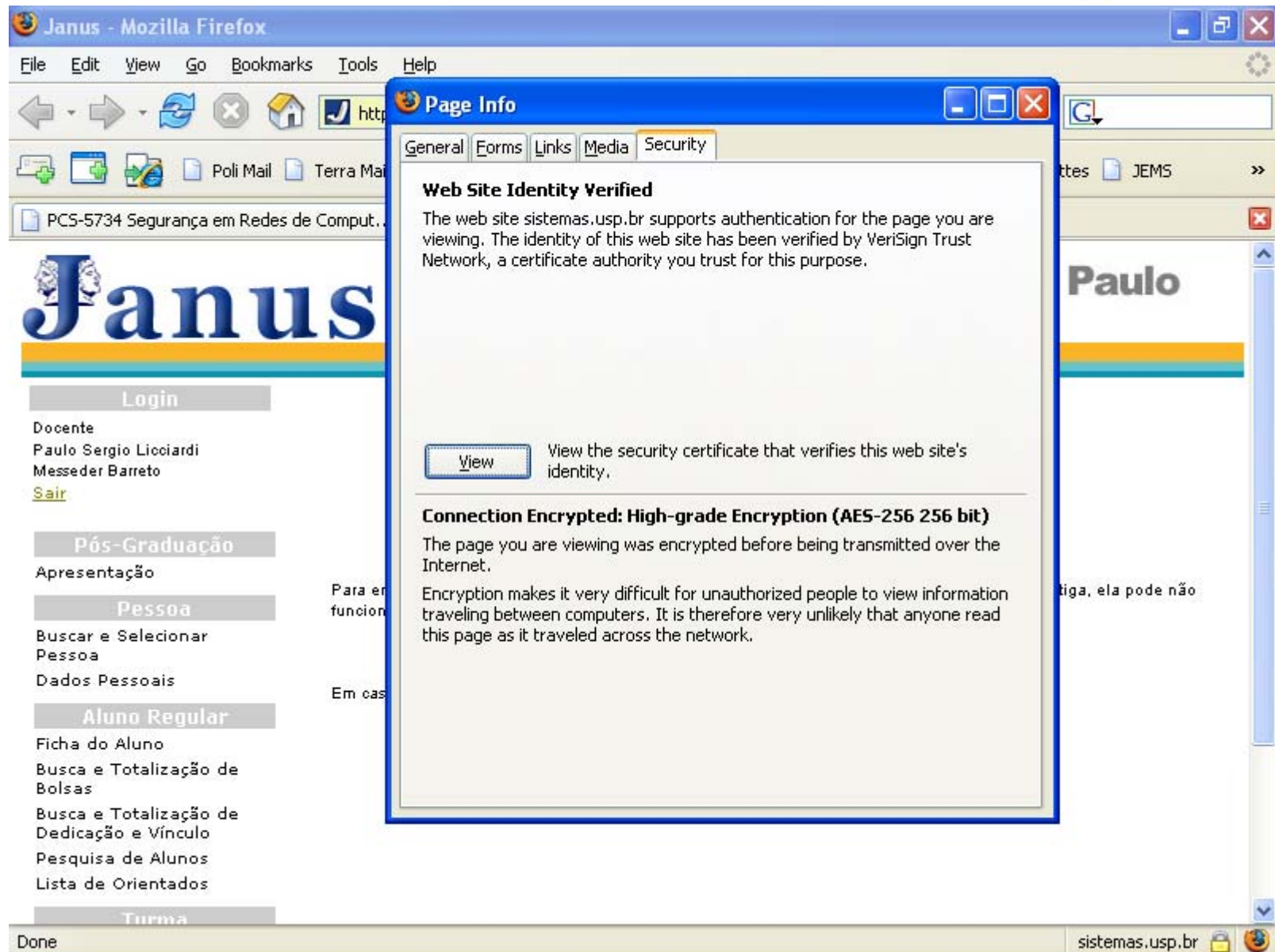
- Versão e número serial.
- Identificação da AC (*issuer*).
- Datas do certificado (efetivação e expiração).
- Identificação da EF (*subject*).
- Chave pública da EF.
- Extensões.
- Assinatura digital da AC sobre todos os dados anteriores.

Distinguished Name

- Globalmente único (em princípio)
- Níveis hierárquicos (separados por "/").
 - Country Name "C=..."
 - State or Province Name "SP=..."
 - Locality Name "L=..."
 - Organization Name "O=..."
 - Organizational Unit Name "OU=..."
 - Common Name "CN=..."
- Identificador único opcional.

ASN.1

- Abstract Syntax Notation One (ASN.1): linguagem de especificação de objetos abstratos – norma X.208.
- Representação serializada: Basic Encoding Rules (BER), Distinguished Encoding Rules (DER) – norma X.209.
- B. S. Kaliski Jr. "A Layman's Guide to a Subset of ASN.1, BER, and DER", RSA Laboratories Technical Note, 1993.



The screenshot shows a Mozilla Firefox browser window with the address bar displaying 'http://sistemas.usp.br'. The main content area shows the 'Janus' website header and a navigation menu with links like 'Login', 'Pós-Graduação', 'Pessoa', 'Aluno Regular', and 'Turma'. A 'Page Info' dialog box is open, showing the 'Security' tab. The dialog contains the following text:

Web Site Identity Verified
 The web site sistemas.usp.br supports authentication for the page you are viewing. The identity of this web site has been verified by VeriSign Trust Network, a certificate authority you trust for this purpose.

[View](#) View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (AES-256 256 bit)
 The page you are viewing was encrypted before being transmitted over the Internet.
 Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

The status bar at the bottom of the browser window shows 'Done' and the address 'sistemas.usp.br'.

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Licciardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

Version 3

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Licciardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPs Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number**
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

22:C4:20:6B:30:9D:C1:B7:4B:7D:E6:D9:25:14:60:2E

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Licciardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPs Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm**
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

PKCS #1 SHA-1 With RSA Encryption

Close


tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Fire
File Edit View Go B
← → ↻
PCS-5734 Segurança em



Login
Docente
Paulo Sergio Lioardi
Messeder Barreto
Sair

Pós-Graduação
Apresentação

Pessoa
Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular
Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

```

OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY
LTD.(c)97 VeriSign
OU = VeriSign International Server CA - Class 3
OU = VeriSign, Inc.
O = VeriSign Trust Network

```

Close


tes JEMS

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Fire...
File Edit View Go B...
< > ↺
+ + + + +
PCS-5734 Segurança em...



Login
Docente
Paulo Sergio Licciardi
Messeder Barreto
[Sair](#)

Pós-Graduação
Apresentação

Pessoa
Buscar e Selecionar Pessoa
Dados Pessoais

Aluno Regular
Ficha do Aluno
Busca e Totalização de Bolsas
Busca e Totalização de Dedicção e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"
General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

```

2007-02-11 21:00:00
(2007-02-12 00:00:00 GMT)

```

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Licciardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- sistemas.usp.br
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

Field Value

2008-02-12 20:59:59
(2008-02-12 23:59:59 GMT)

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Lioiardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- Validity
 - Not Before
 - Not After
- Subject**
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions
 - Certificate Basic Constraints

Field Value

```
CN = sistemas.usp.br
OU = Terms of use at www.verisign.com/rpa (c)00
OU = Centro de Tecnologia da Informacao
O = IMPRENSA OFICIAL DO ESTADO S A IMESP
L = Sao Paulo
ST = Sao Paulo
C = BR
```

Close


tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Fire...
File Edit View Go B...
← → ↻
PCS-5734 Segurança em...



Login
Docente
Paulo Sergio Lioiciardi
Messeder Barreto
[Sair](#)

Pós-Graduação
Apresentação

Pessoa
Buscar e Selecionar Pessoa
Dados Pessoais

Aluno Regular
Ficha do Aluno
Busca e Totalização de Bolsas
Busca e Totalização de Dedicção e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"
General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- Validity
 - Not Before
 - Not After
 - Subject
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions
 - Certificate Basic Constraints

Field Value

PKCS #1 RSA Encryption

Close

tes JEMS

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Fire
File Edit View Go B
← → ↻
PCS-5734 Segurança em

Jan

Login
Docente
Paulo Sergio Lioiciardi
Messeder Barreto
Sair

Pós-Graduação
Apresentação

Pessoa
Buscar e Selecionar Pessoa
Dados Pessoais

Aluno Regular
Ficha do Aluno
Busca e Totalização de Bolsas
Busca e Totalização de Dedicção e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"
General Details

Certificate Hierarchy
Built-in Object Token: Verisign Class 3 Public Primary Certification Authority
OU=www.verisign.com/CPs Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
sistemas.usp.br

Certificate Fields
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Basic Constraints

Field Value
30 81 89 02 81 81 00 b7 10 f2 cf 37 44 33 00 6d
b7 63 89 e1 35 33 d5 a2 ef 2f 92 98 c4 ef 2e ee
90 14 48 69 fd 48 07 8a 89 12 53 a2 ba 51 48 29
ec 92 b3 9f 3f 4d 94 47 bc 11 d3 60 f4 a4 c2 c0
63 f2 68 71 9c fe b5 ae 0f ac a0 a2 e0 02 8e 59
d1 9e 36 79 64 f2 f0 45 10 8b 09 bb f2 f6 64 9d
96 16 8c 0a 46 dd f8 e4 00 10 21 d2 34 f0 ca af
92 3d 4d b6 6a 64 a6 70 3b b5 fe ec 3c 43 9a 36
c3 e5 9f ba 31 98 ad 02 03 01 00 01

Close

tes JEMS
Paulo
ga, ela pode não
sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em

Jan

Login

Docente
Paulo Sergio Lioiciardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa
Dados Pessoais

Aluno Regular

Ficha do Aluno
Busca e Totalização de
Bolsas
Busca e Totalização de
Dedicação e Vínculo
Pesquisa de Alunos
Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- Extensions
 - Certificate Basic Constraints
 - Certificate Key Usage**
 - CRL Distribution Points
 - Certificate Policies
 - Extended Key Usage
 - Authority Information Access
 - Object Identifier (1 3 6 1 5 5 7 1 12)
 - Certificate Signature Algorithm

Field Value

Not Critical
Signing
Key Encipherment

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Janus - Mozilla Firefox

File Edit View Go B

← → ↺ ×

Pol

PCS-5734 Segurança em

Janus

Login

Docente

Paulo Sergio Lichardi

Messeder Barreto

[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar Pessoa

Dados Pessoais

Aluno Regular

Ficha do Aluno

Busca e Totalização de Bolsas

Busca e Totalização de Dedicação e Vínculo

Pesquisa de Alunos

Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPs Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSign...
 - sistemas.usp.br

<http://crl.verisign.com/Class3InternationalServer.crl>

Certificate Key Usage

CRL Distribution Points

Certificate Policies

Extended Key Usage

Authority Information Access

Object Identifier (1 3 6 1 5 5 7 1 12)

Certificate Signature Algorithm

Field Value

Not Critical

30 3d 30 3b a0 39 a0 37 86 35 68 74 74 70 3a 2f

2f 63 72 6c 2e 76 65 72 69 73 69 67 6e 2e 63 6f

6d 2f 43 6c 61 73 73 33 49 6e 74 65 72 6e 61 74

69 6f 6e 61 6c 53 65 72 76 65 72 2e 63 72 6c

Close

sistemas.usp.br


Janus - Mozilla Firefox

File Edit View Go B

← → ↻ ×

Pol

PCS-5734 Segurança em



Login

Docente
Paulo Sergio Lioiardi
Messeder Barreto
[Sair](#)

Pós-Graduação

Apresentação

Pessoa

Buscar e Selecionar
Pessoa

Dados Pessoais

Aluno Regular

Ficha do Aluno

Busca e Totalização de
Bolsas

Busca e Totalização de
Dedicação e Vínculo

Pesquisa de Alunos

Lista de Orientados

Turma

Done

Certificate Viewer: "sistemas.usp.br"

General Details

Certificate Hierarchy

- Builtin Object Token: Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=VeriSi...
 - sistemas.usp.br

Certificate Fields

- Certificate Basic Constraints
- Certificate Key Usage
- CRL Distribution Points
- Certificate Policies
- Extended Key Usage
- Authority Information Access
- Object Identifier (1 3 6 1 5 5 7 1 12)
- Certificate Signature Algorithm
- Certificate Signature Value**

Field Value

```

a4 a2 f9 ce 06 c8 b5 ab b6 61 59 d0 74 39 f0 86
a4 93 f7 54 d8 f4 d7 33 4f bf ea 60 d3 ed 9f 9b
7e 46 f1 f3 ec e2 a6 5d 01 d0 74 d7 cf 8e 5c ea
4d d7 a1 8d 42 1c 36 5e ba e1 66 96 63 3f 57 9a
cf cb 26 ed 78 46 5b 05 cf f5 d4 7f 7e 1f b0 9c
0d 83 0a 1b cd 78 e4 eb e2 ef 82 60 8d 53 4c b2
03 d9 33 29 5d 93 14 57 0c 86 ac d5 bb 43 8e 60
ad b5 c7 ca 15 97 9f fc 5d 56 a0 dd 23 46 25 ce
            
```

Close

tes JEMS >>

Paulo

ga, ela pode não

sistemas.usp.br

Utilização do Certificado

- Duas entidades finais intercambiam por um canal qualquer seus certificados obtidos da mesma AC.
- Cada uma das partes pode verificar a autenticidade do certificado da outra parte usando o certificado da AC.
- As partes procedem a um protocolo de identificação e estabelecimento de sessão a partir das chaves públicas nos certificados.

Revogação

- Comprometimento da chave privada da EF.
- Comprometimento da chave privada da AC.
- Notificação pública emitida pela AC: Lista de Certificados Revogados (LCR), ou "lista negra".
- Distribuição periódica (ponto de distribuição).

Lista de Certificados Revogados

- Enumeração de números seriais (apenas certificados revogados ainda não expirados) e suas datas de revogação.
- Identificação da AC.
- Data de efetivação e da próxima atualização da LCR.
- Extensões.
- Assinatura digital da AC sobre todos os dados anteriores.

Serviço de Diretório

- Padrão X.509.
- Consultas a certificados e LCR's de acordo com vários critérios.
- Protocolo padrão: LDAP (Lightweight Directory Access Protocol).

Extensões de Certificado

- X509 versão 3.
- Inadequação dos campos previstos nas versões anteriores.
- Três categorias:
 - Informação sobre chave e política.
 - Atributos de *subject* e *issuer*.
 - Restrições de caminho de certificação.

Informação sobre Chave e Política

- Identificador da chave da AC.
- Identificador da chave da EF.
- Utilização da chave.
- Período de uso da chave privada.
- Políticas de certificado (remoção de ambigüidades).
- Equivalência de políticas (em certificação cruzada).

Atributos de *Subject* e *Issuer*

- Nome alternativo do *subject* (formatos usados por aplicações específicas).
- Nome alternativo do *issuer*.
- Atributos de diretório do *subject*.

Restrições de Caminho de Certificação

- Certificação cruzada.
- Restrições básicas (atuação do *subject* como AC e limite de caminho de certificação).
- Restrições de nome (formato dos nomes de *subject* em certificados subseqüentes num caminho de certificação).
- Restrições de política (requerimentos de identificação explícita ou inibição de política para o caminho de certificação).

Utilização de Chave

- Assinatura digital.
- Irretratabilidade.
- Cifração de chave.
- Cifração de dados.
- Negociação de chave.
- Verificação de assinatura de AC para certificados.
- Verificação de assinatura de AC para LCR.

Importância de *timestamp*

- Ataques de repetição: um agressor poderia causar danos apenas repetindo mensagens, mesmo sem saber seu conteúdo (no pior caso, poderia fazer-se passar com sucesso por uma das partes da comunicação).
- *Timestamps* garantem irrepetibilidade das mensagens. Limitação: poderia haver repetição dentro do prazo de validade do timestamp (o prazo de validade é necessário para contemplar o reenvio de mensagens por perda de pacotes).

Importância de *timestamp*

- Os *nonces* aleatórios devem ser únicos dentro do prazo de validade de um *timestamp*.
- *Timestamps* precisam ser armazenados apenas durante seu prazo de validade, juntamente com o *nonce* associado.
- Uma mensagem com *timestamp* repetido e *nonce* diferente é um reenvio. Uma mensagem com *timestamp* repetido e *nonce* igual é uma tentativa (frustrada) de ataque.

ICP-Brasil

- Infra-Estrutura de Chaves Públicas do Brasil.
- Medida Provisória 2.200-2 (24 de agosto de 2001).
- Institui a ICP Brasil visando validade jurídica (autenticidade, integridade) de documentos em forma eletrônica que utilizem certificação digital, bem como a realização de transações eletrônicas seguras.

ICP-Brasil



AC-Raiz

AC-SRF

AC-PR

AC-IMESP

AC-Serasa

AC-Jus

AC-Serpro

AC-CEF

Certisign

AC-SRF

AR-PR

AR-IMESP

AC-Serasa

AC-Jus

AC-Serpro

AC-CEF

Certisign

AR-SRF



imprensaoficial

AR-Serasa

AR-Jus

AR-Serpro

AR-CEF

AR-Certisign



Medida Provisória 2.200-2

- Autoridade gestora de políticas: função exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República com representantes da sociedade civil, setores interessados e por alguns órgãos ligados ao governo federal.
- Competências principais do Comitê Gestor da ICP-Brasil definidas a seguir.

Medida Provisória 2.200-2

- Compete ao Comitê Gestor da ICP-Brasil:
 - (*Art. 4, item II*) Estabelecer a política, os critérios e as normas técnicas para o *credenciamento* das ACs, das ARs e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação.
 - (*Art. 4, item VI*) Aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o *funcionamento* das ACs e das ARs, bem como autorizar a AC Raiz a emitir o correspondente certificado.

Medida Provisória 2.200-2

- (Art. 5) À AC Raiz, primeira autoridade da cadeia de certificação, executora das políticas e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os *certificados das ACs de nível imediatamente subsequente* ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de *fiscalização e auditoria* das ACs e das ARs e dos prestadores de serviço habilitados pela ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP- Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
- § único: É *vedado* à AC Raiz emitir certificados para o *usuário final*.

Medida Provisória 2.200-2

- (Art. 6, § único) O par de chaves criptográficas será gerado *sempre pelo próprio titular* e sua chave privada de assinatura será de seu *exclusivo controle, uso e reconhecimento*.
- Obs.: este artigo traz uma consequência jurídica *sutil mas grave*.



Medida Provisória 2.200-2

- (Art. 7) Às ARs, entidades operacionalmente vinculadas a determinada AC, compete *identificar e cadastrar usuários na presença destes*, encaminhar solicitações de certificados às AC e manter registro de suas operações.
- (Art. 8) Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, *poderão ser credenciados como AC e AR* os órgãos e as entidades públicas e as pessoas jurídicas de direito privado.

Medida Provisória 2.200-2

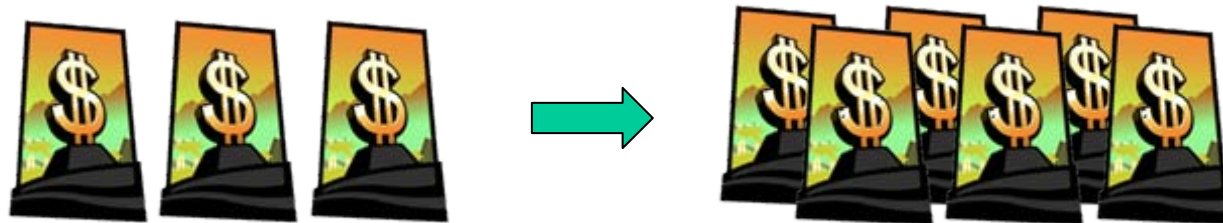
- (Art. 10, § 2) O disposto nesta Medida Provisória *não obsta* a utilização de *outro meio* de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que *admitido pelas partes como válido* ou aceito pela pessoa a quem for oposto o documento.

Resolução nº 13

- 26 de Abril de 2002.
- (Artigo 7.1.2) – Extensões de certificado – Key Usage:
 - Em certificados de *assinatura*, somente os bits `digitalSignature`, `nonRepudiation` e `keyEncipherment` podem estar ativados.
 - Em certificados de *sigilo*, somente os bits `keyEncipherment` e `dataEncipherment` podem estar ativados.

Resolução n° 13

- Em outras palavras, certificados para *assinatura* e certificados para *sigilo* devem ser necessariamente *distintos*.
- Impacto sobre o SPB: *dois* certificados deveriam ser empregados por cada entidade financeira onde originalmente se previa apenas *um*, com todos os custos envolvidos.



Sigilo?

- Certificados e LCRs, e informação corporativa ou pessoal que apareçam neles em diretórios públicos, *não são considerados informações públicas*.
- Todas as outras informações pessoais ou corporativas mantidas pela AC ou uma AR não podem ser divulgadas sem consentimento prévio do usuário, a menos que por determinação judicial.
- Se uma LCR não for pública, como poderá ser verificada?

Guarda da Chave Privada

- A chave privada de assinatura digital de cada usuário deve ser mantida somente pelo usuário, devendo este assegurar seu sigilo. *Qualquer divulgação da chave privada de assinatura pelo usuário será de sua inteira responsabilidade.*
- No caso do comprometimento da chave privada de assinatura digital de um usuário dos serviços da ICP-Brasil, o usuário deverá notificar *imediatamente* a AC que emitiu o certificado.

Guarda da Chave Privada

- Se a chave de um usuário for comprometida sem o seu conhecimento (a detecção não é, via de regra, imediata), como ele pode ser responsabilizado?
- Se houver o comprometimento de uma chave mas o usuário conseguir relatar o ocorrido em tempo hábil para possibilitar a revogação, mesmo assim ele será responsabilizado?

Tipos de Certificado

- A1 até A4 para assinatura.
- S1 até S4 para sigilo.
- Níveis diferenciados segundo a finalidade e os requisitos de segurança associados.

Certificado tipo A1 ou S1

- Chaves geradas por software (e.g. Cryptographic Service Provider do navegador) na estação solicitante. A chave privada é armazenada cifrada por senha no HD da estação, ou em smart cards ou tokens sem capacidade de geração de chaves.
- Chave privada RSA de 1024 bits.
- Período máximo de validade: 1 ano.

Certificado tipo A2 ou S2

- Chaves geradas em smart cards ou tokens com capacidade de geração de chaves criptográficas. Os certificados de equipamentos são gerados em hardware criptográfico instalado no próprio equipamento.
- Armazenamento pode ser em smart cards ou tokens sem capacidade de geração de chaves.
- Chave privada RSA de 1024 bits.
- Período máximo de validade: 2 anos.

Certificado tipo A3 ou S3

- Chaves geradas e armazenadas em smart cards ou tokens com capacidade de geração de chaves criptográficas. Os certificados de equipamentos são gerados em hardware criptográfico instalado no próprio equipamento.
- Chave privada RSA de 1024 bits.
- Período máximo de validade: 3 anos.

Certificado tipo A4 ou S4

- Chaves geradas e armazenadas em smart cards ou tokens com capacidade de geração de chaves criptográficas. Os certificados de equipamentos são gerados em hardware criptográfico instalado no próprio equipamento.
- Chave privada RSA de 2048 bits.
- Período máximo de validade: 3 anos.

Processo de Registro

- Certificados de pessoas físicas:
 - Presença física do interessado com documentos pessoais de identificação (originais + cópias).
 - Titular assina o Termo de Titularidade; AR verifica e recolhe cópias dos documentos de identificação e presencia a assinatura do Termo de Titularidade.
- Exemplo – SRF:
 - Cédula de identidade, CPF, comprovante de residência, PIS/PASEP, título de eleitor.
 - CPF é consultado *on-line* na base da SRF.

Processo de Registro

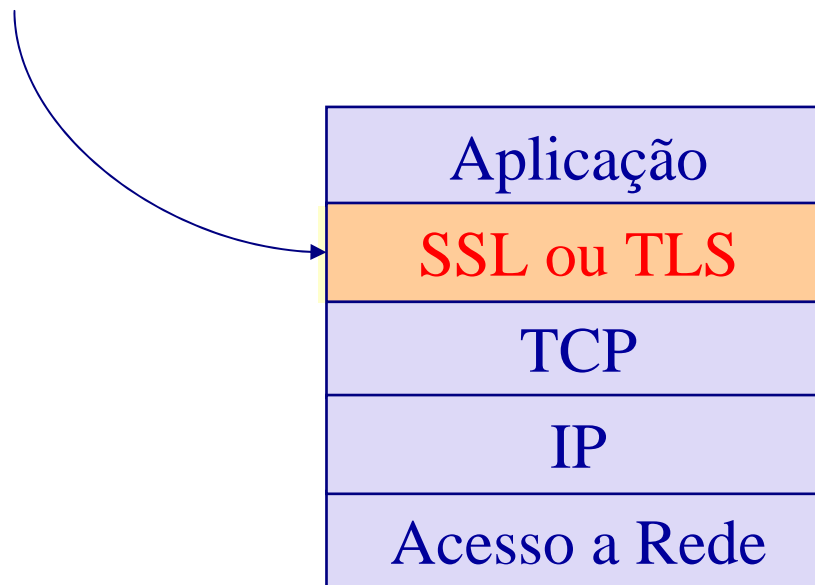
- Certificados de pessoas jurídicas, equipamentos ou aplicações:
 - Presença física do responsável com documentos de identificação.
 - Titular assina o Termo de Titularidade. AR verifica e recolhe cópias dos documentos de identificação e presencia a assinatura do Termo de Titularidade.
- Exemplo – SRF:
 - CNPJ, registro comercial (empresa individual), ato constitutivo ou estatuto ou contrato social (sociedades comerciais ou civis), documentos de eleição de administradores (sociedades por ações).
 - CNPJ é consultado *on-line* na base da SRF.

Apêndice

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL)

- SSL × Pilha TCP/IP
- Camada SSL



Secure Sockets Layer (SSL)

- Duas subcamadas:

Sessão:

Handshake

Change
Cipher Spec

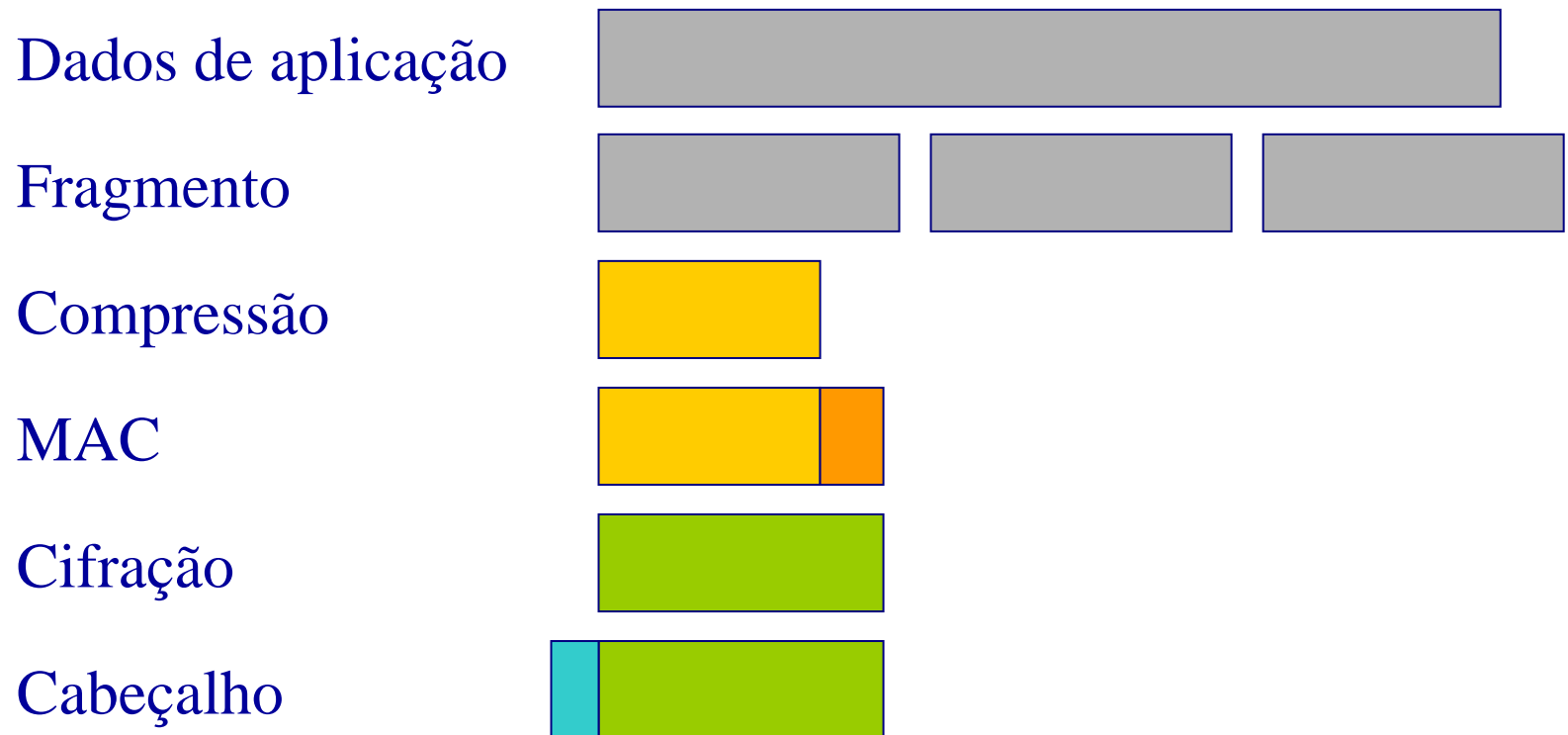
Alert

HTTP

Conexão:

SSL Record Protocol

SSL Record Protocol



Change Cipher Spec

- CipherAlgorithm
- MACAlgorithm
- CipherType
- IsExportable
- HashSize
- KeyMaterial
- IVSize

Change Cipher Spec

Cifras de bloco:

–IDEA

–RC2

–DES

–3DES

–Skipjack

Funções de hash:

–MD5

–SHA-1

Cifras de mascaramento:

–RC4™

Cifras assimétricas:

–RSA

–Diffie-Hellman

–Forteza

SSL Alert

- Dois níveis de gravidade:
 - Advertência
 - Fatal
- Fatal:
 - Encerra a conexão corrente.
 - Outras conexões podem continuar.
 - Nenhuma outra conexão pode ser estabelecida na sessão corrente

SSL Alert

- Erros fatais:
 - Unexpected_message
 - Bad_record_mac
 - Decompression_failure
 - Handshake_failure
 - Illegal_parameter
 - Close_notify
 - No_certificate
 - Bad_certificate
 - Unsupported_certificate
 - Certificate_revoked
 - Certificate_expired
 - Certificate_unknown

SSL Handshake

- Fase 1: Estabelecimento de parâmetros de segurança.
 - versão do protocolo
 - ID de sessão
 - algoritmos criptográficos
 - método de compressão
 - números aleatórios.

Cliente



client_hello

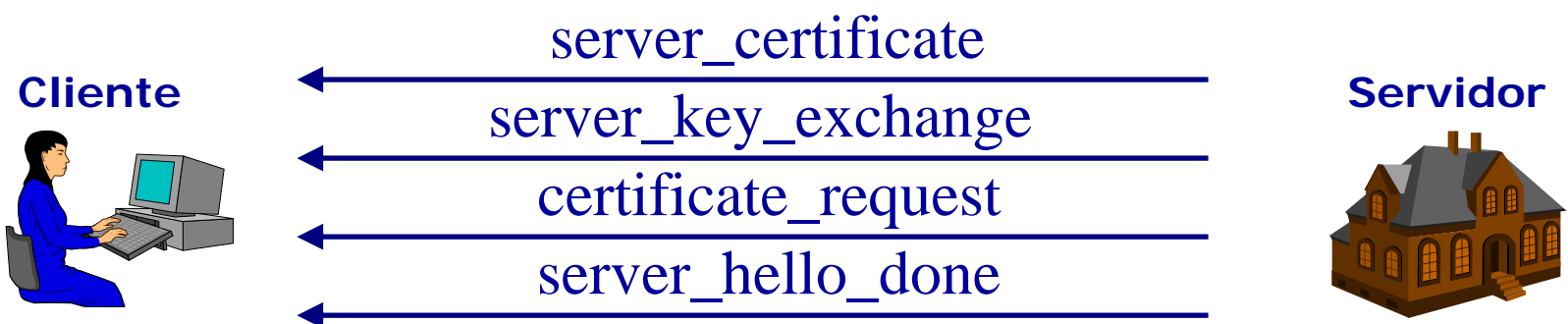
Servidor



server_hello

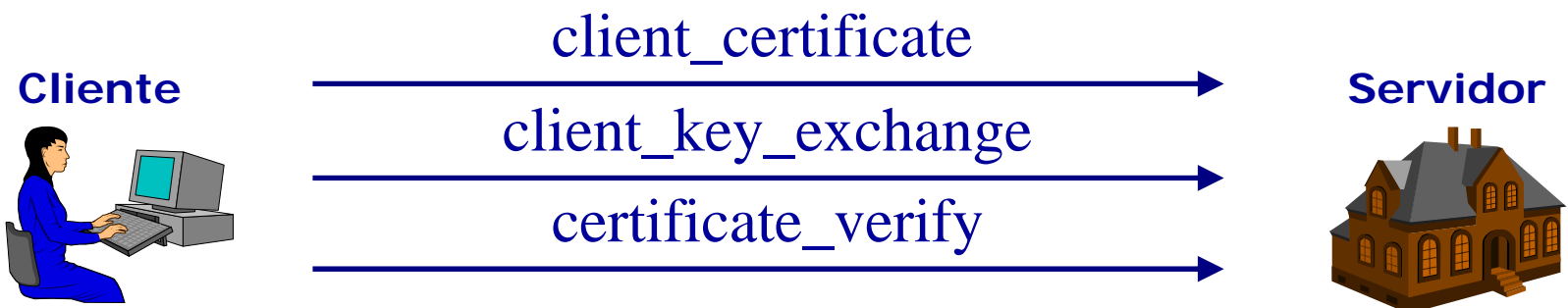
SSL Handshake

- Fase 2: Transmissão do servidor.
 - certificado.
 - elemento assinado de negociação de chave
 - (opcional SSL v3) solicitação de certificado do cliente.



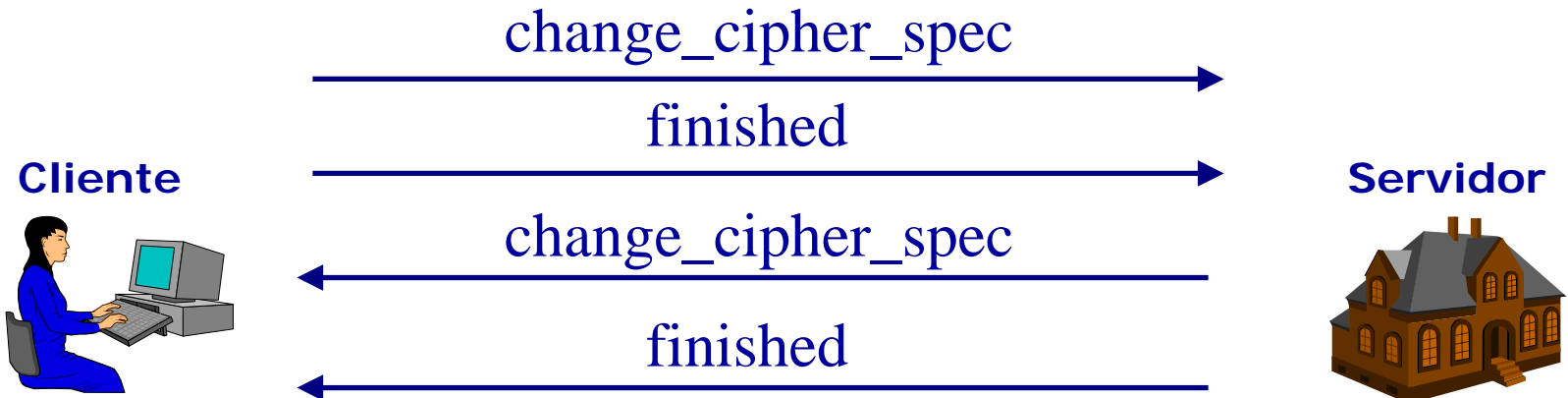
SSL Handshake

- Fase 3: Transmissão do cliente.
 - certificado (se solicitado – SSL v3)
 - elemento de negociação de chave (opcionalmente assinado)



SSL Handshake

- Fase 4: Alteração (opcional) de algoritmos e encerramento.
- Cálculos finais: chave mestra, parâmetros (IVs, chaves de MAC).



Outros protocolos

- IPSec
- SET
- VISA 3D
- Sistemas avançados: criptografia baseada em identidades.

Estudo de Caso: SET

- SET (Secure Electronic Transaction): VISA e Master Card.
- Diferença entre aplicação segura cliente-servidor (SSL) e comércio eletrônico (SET): transações com *múltiplas partes*.
- Outra diferença: especificação com ~800 páginas (vs. ~30 páginas do SSL).

Participantes

<i>Consumidor</i>	Portador do cartão de pagamento
<i>Emissor</i>	Entidade financeira que emitiu o cartão de pagamento
<i>Comerciante</i>	Entidade que oferece bens a venda ao consumidor
<i>Adquirente</i>	Entidade que captura as transações de pagamento
<i>Autoridade Certificadora</i>	Entidade que atesta a identidade dos participantes

SET: Pagamento

