



UNIVERSIDADE FEDERAL DE UBERLÂNDIA  
FACULDADE DE ENGENHARIA ELÉTRICA



## **Atividade Prática 6: Certificados de Segurança**

[Universidade Federal de Uberlândia – UFU; Faculdade de Engenharia Elétrica – FEELT; Relatório referente à disciplina de Redes de Comunicações II, ministrada pelo Prof. Dr. Éderson Rosa da Silva]

Gabriel Andrade Queiroz	11711ETE010
Samuel Alves Tavares	11711ETE008
Lucas Albino Martins	12011ECP022

Uberlândia - MG

2021

## Sumário

1-Certificado SSL	3
2- TLS	4
3- UFU	5
4- Amazon.com	8
5-Referências Bibliográficas	11

## 1-Certificado SSL

O SSL significa “Secure Sockets Layer”(camada de Soquete Seguro) e ele é um protocolo de segurança que faz com que o link entre um navegador e um servidor WEB seja criptografado. Muitas empresas adicionam certificados SSL para que as transações e informações dos clientes sejam privadas e seguras.

O SSL é de extrema importância para sites de vendas, pois protege os dados bancários e de endereço dos clientes, pois uma compra online , para ser considerada segura, precisa passar por processos de autenticação, criptografia e integridade dos dados.

Um fator interessante para de notar, é que sites com certificação SSL utilizam HTTPS ao invés do HTTP na sua URL e também é exibido um cadeado no site, e nele é possível ver mais informações da certificação como para quem ele foi emitido, quem emitiu, sua validade e os motivos, além de ser possível acessar a declaração completa do emissor do certificado

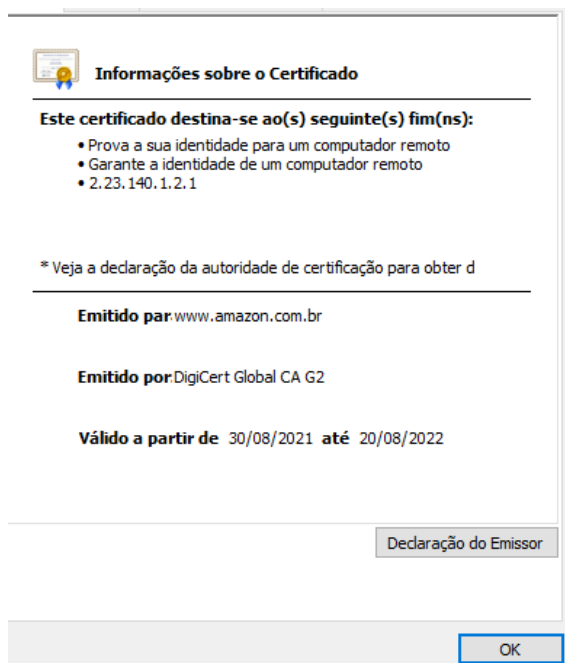


Figura 1- Certificação do site amazon.com.br

Os certificados SSL podem conter vários níveis de validação, por isso são divididos em seis tipos:

- SSL EV (Certificado de Validação Estendida)
- SSL DV(Certificado de Validação de domínio)
- MDC (Certificado de múltiplos domínios)
- UCC ( Certificado de Comunicações Unificadas)
- SSL OV(Validação de Empresa)
- Certificado Curinga.

## 2- TLS

Com a evolução dos certificados, foi criado o TLS(Camada de Transporte de Segurança) para ser o sucessor do SSL,também se trata de um protocolo de segurança para as comunicações sobre as redes de computadores, tendo versões 1.0,1.1 e 1.2. O TLS e o SSL tem suas diferenças, que podem ser vistos na figura abaixo:

SSL	TLS
Seu significado é “camada de segurança de soquete”.	Seu significado é “segurança da camada de transporte”.
A Netscape desenvolveu a primeira versão do SSL em 1995.	A primeira versão do TLS foi desenvolvida pela Internet Engineering Taskforce (IETF) em 1999.
SSL é um protocolo criptográfico que usa conexões explícitas para estabelecer uma comunicação segura entre o servidor e o usuário.	O TLS também é um protocolo criptográfico, porém que fornece comunicação segura entre servidor e usuário por meio de conexões implícitas, sendo considerado, assim, o sucessor do SSL.
Teve um total de três versões lançadas: SSL 1.0, 2.0 e 3.0.	Possui quatro versões lançadas: TLS 1.0, 1.1, 1.2 e 1.3.
Todas as versões foram consideradas vulneráveis e descontinuadas.	O TLS 1.0 e 1.1 foram considerados obsoletos em março de 2020. O TLS 1.2 é a versão que mais tem sido implantada até então.

Figura 1: Diferenças entre o SSL e o TLS.

Vale ressaltar, que no TLS a conexão é segura, pois é utilizada uma criptografia simétrica, e suas chaves são exclusivas para cada sessão iniciada, e sua autenticação pode ser feita através da chave pública, enquanto os arquivos são transmitidos por uma chave privada.

Como pode ser visto, é de extrema importância que sites utilizem os protocolos SSL e TLS para que possam ser considerados seguros, e para mostrar isso, é necessário que os mesmos tenham as Certificações. Para obtê-las, é necessário gerar um CSR, que é um arquivo criptografado com as informações necessárias para a solicitação, como o nome do servidor, da empresa, o setor, a localidade e o código do país com dois caracteres.

Com esse arquivo em mãos, é possível solicitar o seu certificado em diversos locais, basta enviar o arquivo, a solicitação e o pagamento, e o serviço irá validar e lhe enviar o certificado, e o mesmo deve ser instalado no servidor do site.

Para este trabalho, foram selecionados dois domínios diferentes e suas certificações foram analisadas. Para isso, foi utilizada a ferramenta do navegador, ilustrada na figura 1, e o site <https://www.ssllabs.com/>, que faz testes e análises das certificações mantidas pelos domínios inseridos.

### 3- UFU

Foi acessado o site da UFU, com domínio <https://ufu.br/>, e ao clicar no cadeado do HTTPS, foi possível encontrar as informações do Certificado.

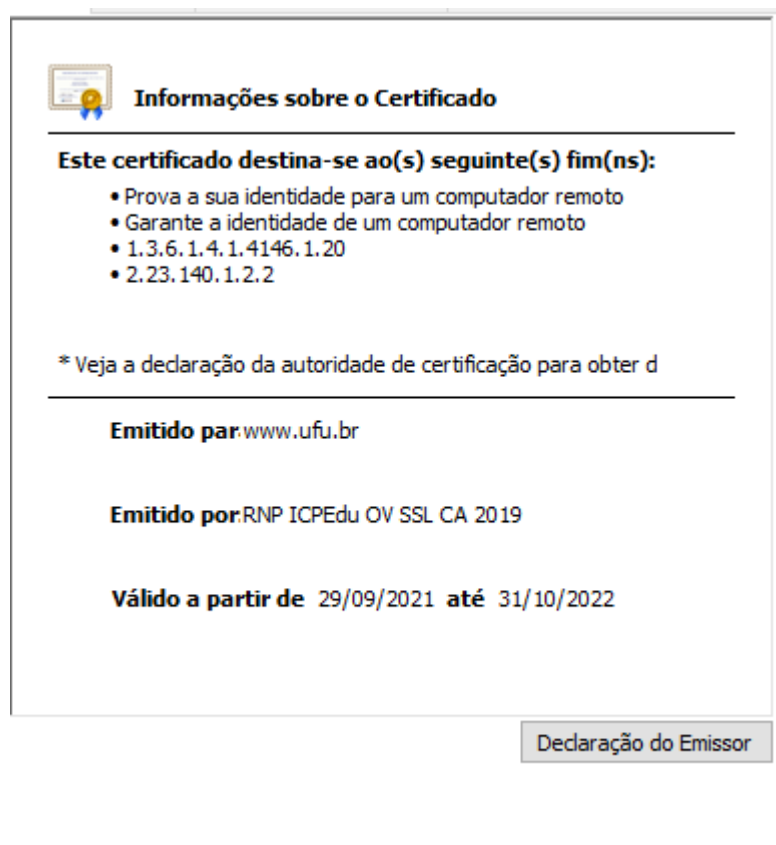


Figura 1- Certificado do domínio <https://ufu.br/>

Sobre o Certificado do mesmo, é possível notar que ele tem sido recentemente validado, e que foi emitido pelo site <https://pessoal.icpedu.rnp.br/home>, que é ligado à Rede Nacional de Ensino e Pesquisa, que faz certificados pessoais e para as comunidades Acadêmicas Federadas.

Após visto as informações básicas do certificado, foi selecionado para ver os detalhes da certificação.

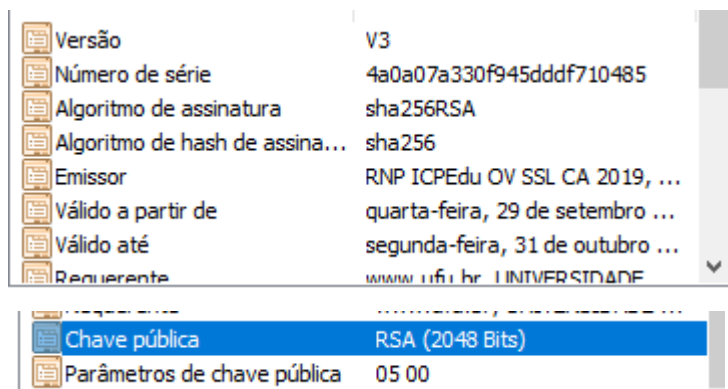


Figura 2- Detalhes da Certificação do domínio 1.

Sobre os detalhes, é importante notar que ela usa um SSL V3, e confirma os períodos de validade.

Outro ponto que é preciso ressaltar é sobre o Algoritmo de Assinatura, que no caso é o sha256. Ele é da família dos SHA-2 (algoritmo de Hash Seguro), são funções hash projetadas pela Agência de Segurança Americana (NSA), e que tem o objetivo de gerar hashes com base de um padrão para qual os dados possam ser protegidos contra qualquer ataque ou agente externo que queira modificá-los. O número 256 representa o número de bits, que podem variar entre 224,256,384 e 512.

Também, foi possível notar que o domínio utiliza uma chave pública do tipo RSA (Rivest-Shamir-Adleman), que foi um dos primeiros sistemas de chave pública, e sua encriptação de chaves é diferente entre a chave pública e a chave privada. A chave estudada, tem um tamanho de 2048 bits.

Após , foi selecionado o caminho que a certificação faz até o domínio 1, passando pelo GlobalSign Root, Trusted Root, o RNP ICPEdu e então indo para a UFU.

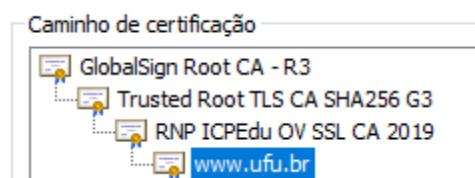


Figura 3- Caminho da Certificação do domínio 1.

Após feita a análise do certificado pela Plataforma do Navegador, foi utilizada a avaliação do SSL Labs, da qual foi possível encontrar outras informações importantes.

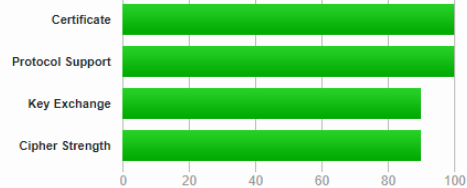
## SSL Report: ufu.br (200.19.145.55)

Assessed on: Sun, 03 Oct 2021 23:57:26 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Figura 4- Avaliação da Certificação do domínio 1

No Report enviado, foi possível avaliar a qualidade do SSL do domínio, que no caso da UFU, recebeu uma média A, o que é excelente, e que utiliza um protocolo TLS (Camada de Transporte de Segurança) 1.2, que é um algoritmo mais seguro quando comparado ao TLS 1.0 e TLS 1.1 .

Foi possível, além disso, obter informações sobre os certificados, como o número serial e as validades, além do Algoritmo e da Chave e seu tamanho, além de outros certificados, que não o principal, como pode ser visto nas figuras 5 e 6:

### Certificate #1: RSA 2048 bits (SHA256withRSA)



#### Server Key and Certificate #1

Subject	www.ufu.br Fingerprint SHA256: 9f3b6890692e00b39a1d25fa77074df53f9e42857b2c1f004175edc6b495e2c Pin SHA256: MhDrutdCyg+4plGuoh49IZiaYK1JcpCeK0W3+lJmaT4=
Common names	www.ufu.br
Alternative names	www.ufu.br ufu.br
Serial Number	4a0a07a330f945dddf710485
Valid from	Wed, 29 Sep 2021 19:31:04 UTC
Valid until	Mon, 31 Oct 2022 19:31:04 UTC (expires in 1 year)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RNP ICPEdu OV SSL CA 2019 AIA: http://secure.globalsign.com/cacert/impicpeduovssca2019.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.globalsign.com/impicpeduovssca2019.crl OCSP: http://ocsp.globalsign.com/impicpeduovssca2019

Additional Certificates (if supplied)	
Certificates provided	3 (4205 bytes)
Chain issues	None
#2	
Subject	RNP ICPEdu OV SSL CA 2019 Fingerprint SHA256: 88fc18bd071be1fbc53ffbc801f03f5b2c4da87bba0c098e2b4808f19eab05fe Pin SHA256: 34rLDmx5N4iFlu/FTyuZjezXxhR4lhOmxmSZ9Pjypro=
Valid until	Fri, 15 May 2026 00:00:00 UTC (expires in 4 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	Trusted Root TLS CA SHA256 G3
Signature algorithm	SHA256withRSA
#3	
Subject	Trusted Root TLS CA SHA256 G3 Fingerprint SHA256: 91119ce503c9fe7f9587d8efbef7315aeee77dc2d14526126493b4ad6fe801f Pin SHA256: hMdlk/Qh87wkhjuY3vWY/C85yuCKrEftb9b3j7xJNPec=
Valid until	Sun, 25 Apr 2027 11:00:00 UTC (expires in 5 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign
Signature algorithm	SHA256withRSA

Figuras 5 e 6 - Avaliação da Certificação do domínio 1

## 4- Amazon.com

Foi realizado o mesmo procedimento do domínio 1, mas agora para o site da Amazon: <https://www.amazon.com.br/>, e também foi possível ver a data de validade, no caso até dia 20/08/2022, a data de emissão, que foi em Agosto deste ano, além do emissor, que foi a empresa DigiCert Global, uma empresa especializada em gerar certificados SSL e TLS.

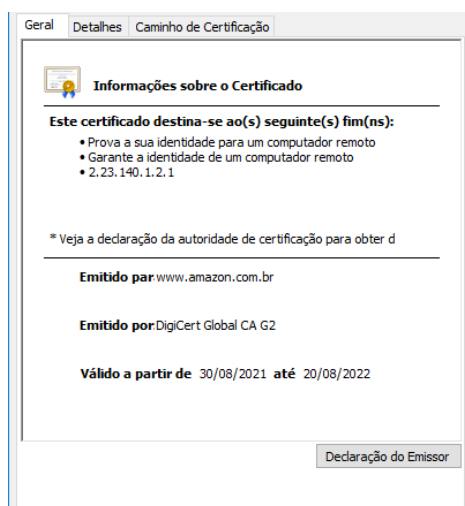


Figura 7: Certificado do domínio 2

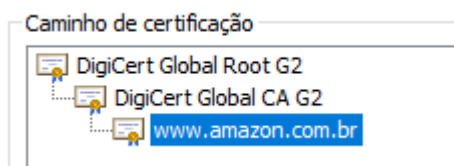
Ao analisar os detalhes dos Certificados, foi notado que ambos utilizaram os mesmos algoritmos, o SHA-256 e uma chave RSA de 2058 bits.



Campo	Valor
Versão	V3
Número de série	0f5bf07f3ddd9aebcc73e0b5f8...
Algoritmo de assinatura	sha256RSA
Algoritmo de hash de assina...	sha256
Emissor	DigiCert Global CA G2, DigiCer...
Válido a partir de	segunda-feira, 30 de agosto d...
Válido até	sábado, 20 de agosto de 2022...
Requerente	www.amazon.com.br

Figura 7: Certificado do domínio 2

Já seu caminho, passou por 3 instâncias: duas na DigiCert e então para a Amazon.



Assim como no primeiro caso, foi analisado o report do SSL Labs para encontrar mais informações.

#### SSL Report: [www.amazon.com.br](https://www.amazon.com.br) (104.119.86.232)

Assessed on: Tue, 12 Oct 2021 14:03:47 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another »](#)

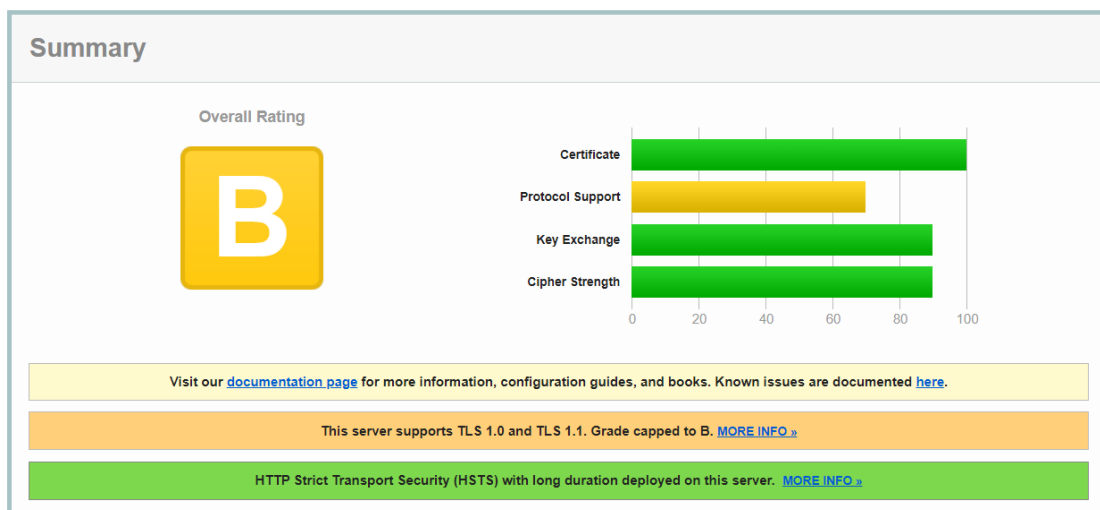







Figura 7: Certificado do domínio 2

O domínio da Amazon recebeu uma nota pior que o da UFU, isso devido a utilizar protocolos antigos, como o TLS 1.1 e 1.0, e não aceitando o TLS1.3.



Nele, também foi possível achar os certificados e chaves, como mostrado nas figuras 8 , 9 e 10:

Certificate #1: RSA 2048 bits (SHA256withRSA)	
<div> <b>Server Key and Certificate #1</b> </div>	
Subject	www.amazon.com.br Fingerprint SHA256: 8f312fcd620b8327ecf529b7b2f93ae487f18848fe68384555a2aff21c5fa9a Pin SHA256: dQP3UCvIFVwT0y1NIB9WSuRkMXb19LHYZPKUnVES5b8=
Common names	www.amazon.com.br
Alternative names	www.cdn.amazon.com.br www.amazon.com.br test-www.amazon.com.br p-yo-www.amazon-com-br-kalias.amazon.com.br p-y3-www-amazon-com-br-kalias.amazon.com.br p-nt-www-amazon-com-br-kalias.amazon.com.br
Serial Number	0e732506ecfa2fb6f3b02823260d8828
Valid from	Mon, 27 Sep 2021 00:00:00 UTC
Valid until	Mon, 26 Sep 2022 23:59:59 UTC (expires in 11 months and 22 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert Global CA G2 AIA: http://cacerts.digicert.com/DigiCertGlobalCAG2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No

<div> <b>Additional Certificates (if supplied)</b> </div>	
Certificates provided	3 (4202 bytes)
Chain Issues	None
#2	
Subject	DigiCert Global CA G2 Fingerprint SHA256: 8fac576439c9fd3ef153b51f9edd0d381b5df7b87559cebeca04297dd44a639b Pin SHA256: njN4rRG+22dNXAi+yb8e3UMypgzPUPHiv4+foULw1g=
Valid until	Tue, 01 Aug 2028 12:00:00 UTC (expires in 6 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root G2
Signature algorithm	SHA256withRSA
#3	
Subject	DigiCert Global Root G2 Fingerprint SHA256: 2d4fad3455ab61397401abbb518922f84336b67e02fc8d2db283825c4ab981bb Pin SHA256: i7WTqTvh0OiolrulfFR4kMPnBqrS2rdVPIs2uC/CY=
Valid until	Sat, 05 Nov 2022 23:59:59 UTC (expires in 1 year and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA256withRSA

		Protocols	
TLS 1.3			No
TLS 1.2			Yes
TLS 1.1			Yes
TLS 1.0			Yes
SSL 3			No
SSL 2			No

		Cipher Suites	
# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	<b>WEAK</b>		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	<b>WEAK</b>		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	<b>WEAK</b>		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	<b>WEAK</b>		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	<b>WEAK</b>		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	<b>WEAK</b>		112

Figuras 8,9 e 10 - Informações sobre os certificados e protocolos do domínio 2.

## 5-Referências Bibliográficas

- [1] Diferença entre SSL e TLS. <https://kinsta.com/pt/base-de-conhecimento/tls-vs-ssl/> , Acesso em 02/10/2021.
- [2] Redes de computadores e a Internet: uma abordagem top-down. Jim Kurose. Pearson, 6ª Edição.
- [3] O que é o TLS?. <https://rockcontent.com/br/blog/tls/>. Acesso em 02/10/2021.
- [4] Amazon. <https://www.amazon.com.br/> . Acesso em 11/10/2021
- [5] SSL Labs. <https://www.ssllabs.com/ssltest/> . Acesso em 11/10/2021
- [6] Universidade Federal de Uberlândia. <https://ufu.br/> . Acesso em 11/10/2021.