



Authentication and Access Control

LEI: Segurança Informática e nas Organizações 2019-2020

89296 | Tomás Batista

88887 | Flávia Figueiredo

Índice

Índice	1
Introdução	2
Desenvolvimento	3
Desenho do Protocolo	3
Autenticação do servidor com Certificados X.509	5
Autenticação do cliente com Senhas	7
Autenticação do cliente com Cartão de Cidadão	9
Mecanismo Controlo de Acesso	12
Mecanismos de Segurança Adicionais	13
Conclusão	14
Bibliografia	14

Introdução

Este trabalho consiste na implementação de um protocolo desenhado pelo grupo para a criação de um canal de comunicação seguro para a troca de um ficheiro de texto entre o cliente e o servidor com autenticação dos intervenientes na comunicação e o controlo de acesso aos clientes.

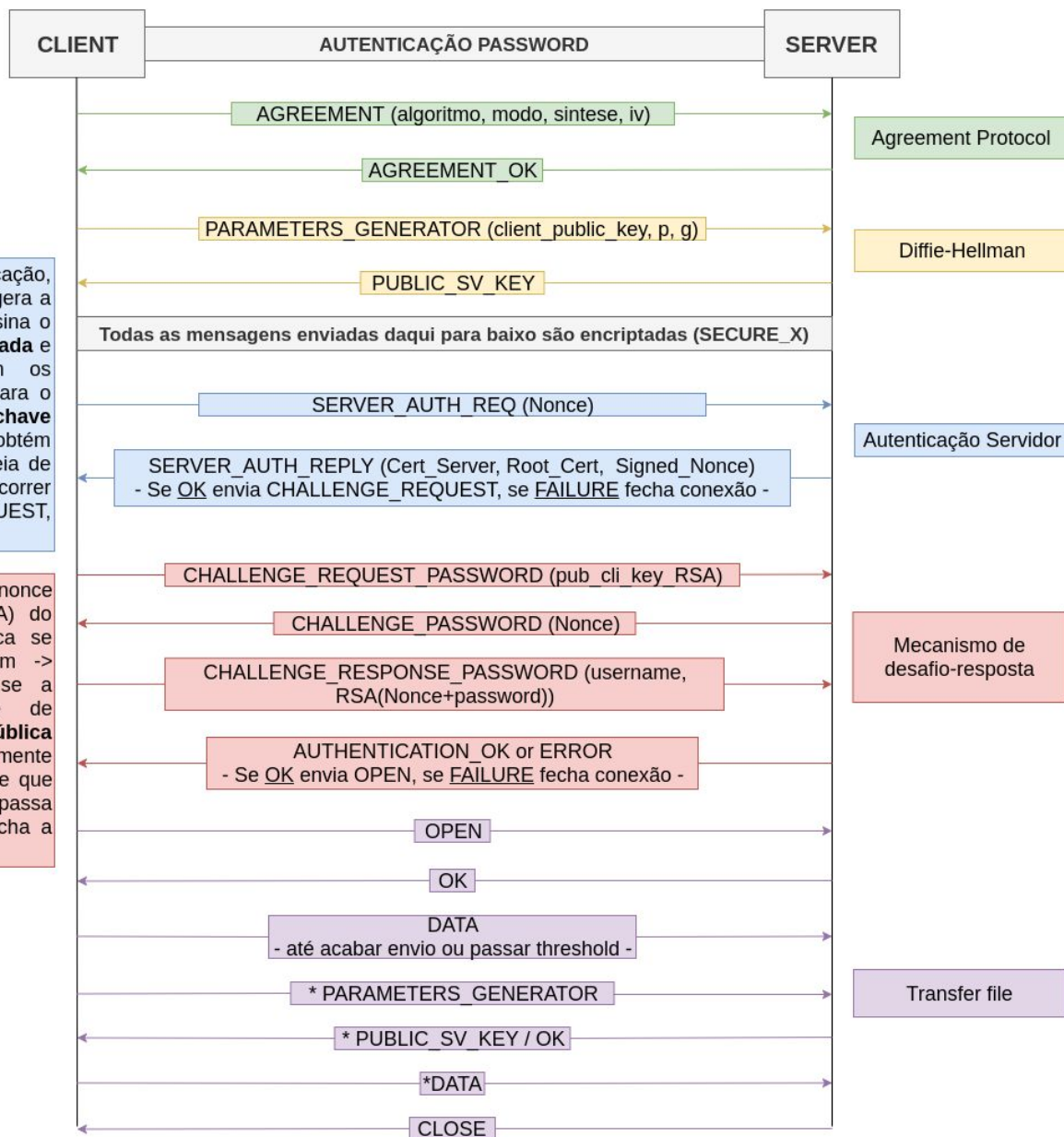
Este projeto tem como base o projeto 03 (Applied Cryptography), do qual foram mantidas a encriptação de mensagens, Diffie-Hellman, MAC para verificação de integridade e o mecanismo de rotação de chaves.

Foram implementados protocolos para a autenticação de utentes através de um mecanismo de desafio resposta, para controlo de acesso, para a autenticação de utentes através do cartão de cidadão, para a autenticação do servidor utilizando certificados X509.

O modo de autenticação a escolher (Password ou CC) é escolhido através de um parâmetro: **-mode CC/PWD**

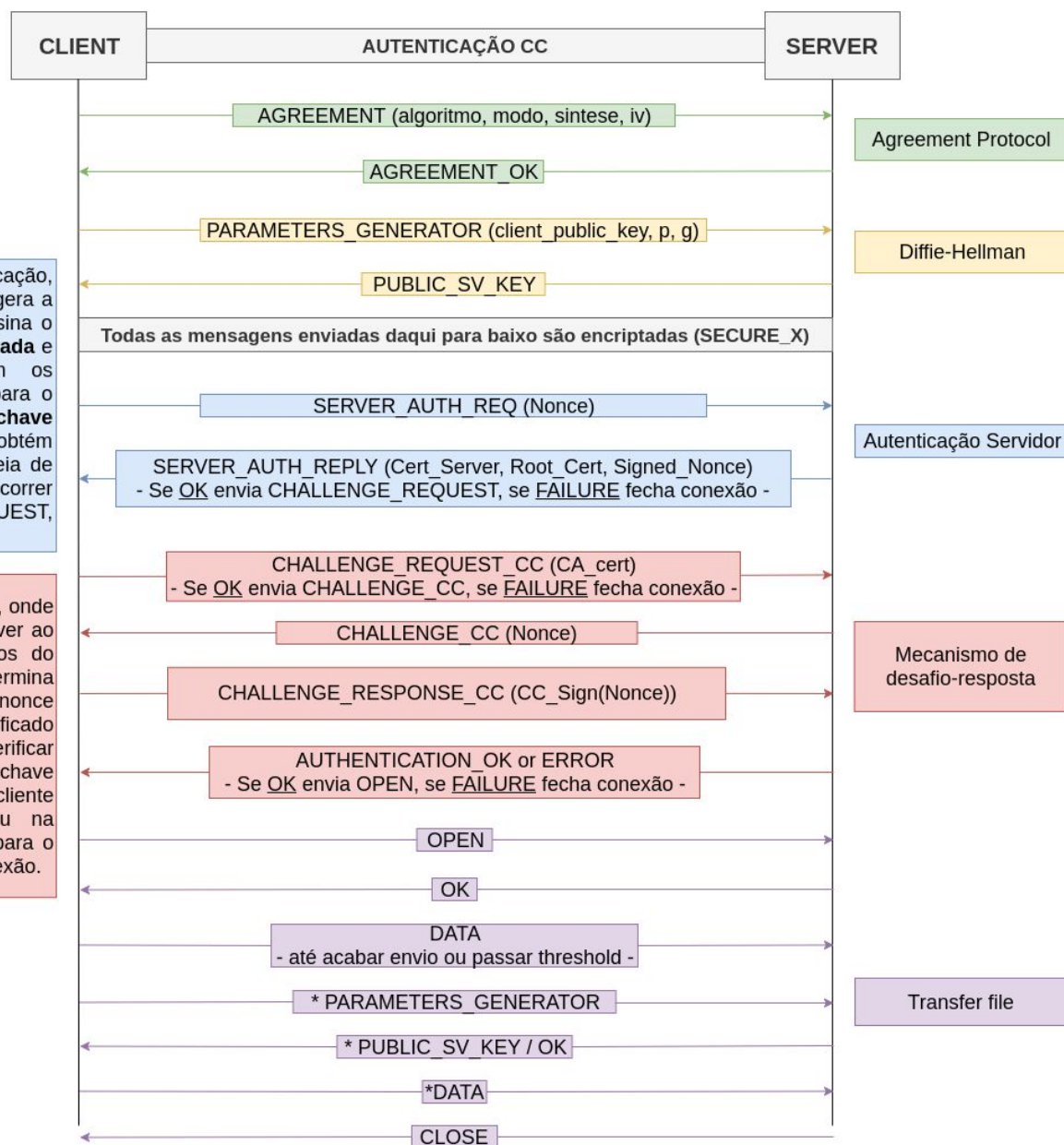
Desenvolvimento

Desenho do Protocolo



* Apenas acontece se o threshold da quantidade de dados enviados não for ultrapassado. Quando for ultrapassado, irá ser gerada nova key. Poderão ser geradas várias keys para um mesmo texto.

Autenticação por apresentação senhas



* Apenas acontece se o threshold da quantidade de dados enviados não for ultrapassado. Quando for ultrapassado, irá ser gerada nova key. Poderão ser geradas várias keys para um mesmo texto.

Autenticação por apresentação do CC

Autenticação do servidor com Certificados X.509

Foram gerados 2 certificados através do XCA, um para a Root CA e outro para o servidor (foram também geradas as chaves privadas destes mesmos certificados). Como é possível observar no desenho do nosso protocolo, após o Diffie-Helman o cliente envia um pedido ao servidor para se autenticar, contendo um nonce.

Ao receber este pedido, o servidor vai carregar o **seu certificado**, o **certificado da sua raiz** e a **chave privada do seu certificado**. Após isto, o nonce recebido pelo cliente é passado por uma função hash (SHA256) e assinado com a sua **chave privada do seu certificado**, usando RSA, e vai enviar de volta para o servidor:

- o seu certificado,
- o certificado da sua raiz,
- o nonce assinado.

Quando receber a resposta do servidor, o cliente vai passar o nonce que tinha enviado anteriormente por uma função hash (idêntica à mencionada anteriormente) e assiná-lo com a **chave pública do certificado do servidor** que vai construir através do certificado do servidor que recebeu na mensagem e vai comparar com o nonce que recebeu que foi assinado pelo servidor com a **chave privada do certificado do servidor**. Se esta verificação falhar, a autenticação do servidor falha e é fechada a conexão.

Caso a autenticação do nonce seja válida, este prossegue para a análise da chain do **certificado do servidor**. Se este, ao analisar a chain, encontrar a root com certificado autoassinado, valida a chain e prossegue para o mecanismo resposta.

```
2019-12-15 06:55:41 Flavia root[9144] INFO New message: {'type': 'SERVER_AUTH_REPLY', 'nonce': 'CLPQ07PmL7MMYK1vzhZMIJfTRD9+gx4jpvTya9zDVn+PmMshZ3/BrC
U62rR7qqj6qdCHP066u4B0JvGUZSA95TaIbQrTepcb+2vqHraofMUNbNAk417UyxKAWDIK75ExqcYQuUSCSgff+Dyqth7IoVncxAxwTAF/iTazgJA8wm0ElhzFDkq1jM/i66Gs8dGzuQvg0QiaE0Sx
tzatioEYBliYnk7Z0mhGkeiyZ1jGbv2q6DQIYSAloB9AnEptgFpu+duKdY0qWxZkcfnFX0okWFNSiUVYLH07crAk1xwYn5z+LEM7g0niENAl6d9FVfychZcumRDJndSHxk4BkpPXqg=', 'server
_cert': 'MIIEJTCCAww2gAwIBAgIIW4I0jQ7hodUwDQYJKoZIhvcNAQELBQAwYExEc2AJBgNVBAYTALBUMQ8wDQYDVQQIEwZBdmVpcM8xDzANBgNVBACTBkF2ZWlybzELMAKGA1UEChMCVUExDTALB
gNVBAsTBERTFVEkxDbzANBgNVBAMTBnJvb3RDQTEjMCEGCSqGSIb3DQEJARYUdG9tYXNlYXRpc3RhOTlAdWEucHQwHhcNMjE0MTY1NjAwWjCBDELMAKGA1UEBHMCFQ
XDZANBgNVBAGTBkF2ZWlybzEPMA0GA1UEBxMGQXZlaXJvMQswCQYDVQQKEwJVQTEENMASGA1UECXMEREVUSTESMBAGA1UEAxMJbG9jYVxob3N0MSMwIQYJKoZIhvcNAQkBFhR0b21hc2JhdGZldGE5O
UB1YS5wdDCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJSewXFjgyo3TGUXNDpL0/vfmS2aADfnHxxU09xQRM2+I4fC//DSGeHGup73BtwVdWP/PsCBX6QaPs0KcJA8eIV2XWshy7O6BHz
r06uFStIOD3f036TMZcj1TOuy57/N0pDFxCRIUhzz4zQjgS7a67PCQSSd46MoJl5lCxaFkxh/kY51zsnInGjmEw+n219kF4SfetUMU0FJ2e5wru88Thwyqf/ZbMniqZwh6Rp0U7ztBaFEXTc5eMrv2
03LamaQQC3pJoJkDiBQaejy7+2jkc7UDUN6bvUue1HAQUdnYOCM9XHL0Xc0DpMpgYVUe4NQKmk7ghody58fvxJV6Cpm4UCAwEAa0BnzCBMDAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWB8TjqqTo7Nw
FHZHoYJmHhnsMfa2/gzALBgNVHQ8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAWewFAYDVR0RBA0wC4IJbG9jYVxob3N0MBEGCWCgSAGG+EIBAQQEAWIGQDAeBgIghkgBhvCAQ0EERYPeGNhIGNlC
nRpZmljYXRlMA0GCsGSIb3DQEBCwUAA4IBAQB3nQ60fa5iSGNDeAhRGLCwweLRzSBGx/upM4xdJNaBYytpNZAAAGaaZ0zrgZL9kjdV0wJahGSUSF2KQjGKDNk8YKYldg6JbJQUj6fkdz00LkkWsdLK
80ekM/k4KqzPs8SandKikEM9gz6CQTWCulkjNpHdMMu8zzQdE3gtcueJoAt1cHSuLFrV10lMJUicatuZiPr6N/00pf9xbcnNZJnInt8AZLAjY7ek3kZJ8oIZIavDfiNvrq6aNMf5jyNIWi96fa6x6q
MqW6IbucKiaclT4feFy6rjj2Dn7MGFBnxM7d+k/UBDMjQKC944Pni2Ak3KcoroWBK8zJRKqtKJwbju'}
2019-12-15 06:55:41 Flavia root[9144] INFO Server Nonce Authenticated
```

Autenticação do servidor

Autenticação do cliente com Senhas

O server tem em memória uma “base de dados” com as credenciais dos usernames.

```
2019-12-15 05:11:34 flavia root[5425] INFO New message: {'type': 'CHALLENGE_PASSWORD', 'nonce': 'YYqbqZNcHcrnBki2XdB35A=='}
2019-12-15 05:11:34 flavia root[5425] INFO Got nonce, going to respond to challenge
Use user, pwd (flavia, flavia) to try a user that its allowed to get the files
Use user, pwd (tomas, tomas) to try a user that its NOT allowed to get the files
Username:
Password:
```

Username e Password

Ao ser selecionada a opção de argumento de autenticação por senhas, este vai ser o modo de autenticação a ser usado.

O desafio mecanismo resposta para a autenticação com senhas inicia-se com o envio de uma mensagem do cliente com um pedido de challenge onde adiciona a **chave pública** usada no RSA. Após isto, o server guarda a chave que foi enviada e envia para o cliente um nonce, ao receber este nonce, são introduzidos o username e password (tal como se pode ver na figura acima), depois a password é concatenada ao nonce e assinadas com a **chave privada**.

Para o servidor são enviados o username e nonce+password assinados.

Ao receber estes, em primeiro lugar, verifica se contém o username, se não contém cancela a conexão e avisa, visto que não há necessidade de tentar validar a password.

Se o username existe, ele vai pegar no nonce que enviou, vai buscar a password do username em questão, vai concatená-las e vai assinar com a chave pública que tinha sido enviada antes pelo cliente. Após assinar, compara a password assinada com a chave privada que recebeu do cliente com a que ele assinou

com a chave pública. Caso sejam iguais, a autenticação está concluída e é prosseguida a troca de mensagens, caso não, é desligada a conexão.

```
2019-12-15 05:13:09 flavia root[5723] INFO New message: {'type': 'CHALLENGE_PASSWORD', 'nonce': 'edp3XjCoR9aFNURDLiG5KA=='}
2019-12-15 05:13:09 flavia root[5723] INFO Got nonce, going to respond to challenge
Use user, pwd (flavia, flavia) to try a user that its allowed to get the files
Use user, pwd (tomas, tomas) to try a user that its NOT allowed to get the files
Username: flavia
Password:
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciDABe1Y/G8hdeMBc9+E00F47ng23J+Nj+Ykupt2rHp273AsDg9rCB
g9uGdczkLbpvJPSl3VcwMuXMNq9KhxOuXdpMpf8mF4MbZjKXdy4q0+yGIFX530i/Ve02iW1HymGebU07LZWU+yNaYJdT+J07JXBD4RTL232FTk62808ep0XXnmGd0RIg4E91PBqBwGVgphByx7I7n
xv4Iesim8vptxKCJSDTCEPBJT1pB9VeXPcwv8o45lmlP0gIRw22lsJHgAuMZNqpKWNn+xQms933L1NZ05d1b6R0GaQ8CKVPZ0YnaedArszeAA/q5o/Ln+JSM5MAZPLRC7Mp71GTsPrhgJw1KIX9kL
xGn2wJVLHc+sZtsrEy5JmQyeYL7abD/xo804pVRaQA593M3mk0ZktfLLNHHj7ZztWp1VWIR432eD3P/A0jYj6AY4JXAZi3r8mSchyzYkkl7JxTDLPljtizw10vvNxsKAWeyeb3TFQu0Yv2kcKUWgk0
RCZDJ4JHiqZlPbw1+3MMumfyxtmxmLWycycTNZ8gLWZHyi8oFGJ84ongSVZ6ggcySta92bryDUQgcBwXMP/IqckjgKe5PF0FXRc5FK6pp0IKgLIIEkfFvNWB4BR5F5VMVINRx7U0rD3biNa3wu6/Ql/
3+03N929AIFnNh9RnFGLDP/Y8pLU0vKdF21T+L4eT29YtwqKzboBckJZOmA3MaI8IGQ9/OVNiLoaZx3gYtQ8XTUXNIQUtnow==', 'HMAC': 'HCjbDWHYCBd3fqKVM++AF1g=='}
2019-12-15 05:13:13 flavia root[5723] INFO New message: {'type': 'AUTHENTICATION_OK'}
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciDd+XNY+kkW2kCS56CyP/A/V0ZhtRCIgm0X71JU++3L/J3eV3emH
X+TehyqklJ/W5yF41TYSw6MA2Kuv6BjmlLjJzFif87XB5QQ5UwIlr4E1WYWGxSmwCf3JXkJwG60i6e0K0kAqIxm0BYtuwaqRW/yOD0bq4U2sT+o7T4Kp5UQtHbkUtyZjk', 'HMAC': '6AVg2sEp
48KetrXfcfnLEw=='}
2019-12-15 05:13:13 flavia root[5723] INFO New message: {'type': 'OK'}
2019-12-15 05:13:13 flavia root[5723] INFO Channel open
2019-12-15 05:13:13 flavia root[5723] INFO Sending file: /home/falacio/Desktop/Authentication-and-Access-Control/requirements.txt
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciC02dwB/BNVBBTvzsZyHh3j7VmKACivURKUeCwVvIr2wNSJUACGB5
RVfKTLljgFD1pA/NVnJUGWgYnQ4ByDddXPu0Gr6VDSe+h2f9blT22cBIsoqpf561eoE7rJdYwKBXTUNp2HFDR3usNKejiTAug8Ugb6Fzy5uIR10ryFLyV6hg0QstEgUdmZRHmMhaVqJ/Z9Yk5tFN
l9Pe3rZNAcSpBsQY/0TFMB8=', 'HMAC': 'EPgEljEwL06GkasC+0x0Ug=='}
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciCKN7HAOfMDNsEBTLlpsm8GkxwwQShM/vA=', 'HMAC': 'LherGH
FnrC8jHYGfeq8KXg=='}
2019-12-15 05:13:13 flavia root[5723] INFO File transferred. Closing transport
2019-12-15 05:13:13 flavia root[5723] INFO The server closed the connection
(venv) falacio@flavia:~/Desktop/Authentication-and-Access-Controls$
```

Autenticação efetuada com sucesso

```
2019-12-15 06:11:36 flavia root[7975] INFO New message: {'type': 'CHALLENGE_PASSWORD', 'nonce': 'jZgqzsLC0xaSZOAAeVJICa=='}
2019-12-15 06:11:36 flavia root[7975] INFO Got nonce, going to respond to challenge
Use user, pwd, secret (flavia, flavia, galinha) to try a user that its allowed to get the files
Use user, pwd, secret (tomas, tomas, ovo) to try a user that its NOT allowed to get the files
Username: flavia
Password:
Qual e coisa qual e ela...: galinha
2019-12-15 06:11:44 flavia root[7975] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'YmBrV9bo+HPqdEucaqn6C/P9XggnMAI3qXrpt/z3UcZe4mrZJgpHHo9/UgclQ
g9YDY5FdMQJvp7TabA2zxd+uwORNCXh8pQGfW53DAIAbSxw/0i+LgpnUz6CsV0xrmSxCLdjJf7Qr9HBMgAkVw7NYwoMxp2dQjvhEuGrdH0W7twYXzvgfRffBzumL7SF7oh2GGsEMLZkSDF1cayMZs2
2aCvCyAcTaS2hag2dcvRsMgEq6py4bDF3gtcVWateCHEBj8j/JNJw7u8UujEX3g6w0YbtomL1MqLn+BokWSIKqOGDBvKyVu3EYRHKLfNf0Z3yCNDK6Lssew9dWlmaUSBF6d2IV2/D4JKE4SgYPggT
dEaLBGxbsmKegatXV895t0Er1ixQNMDpLEIFVRRyqiEVJSb/hw7iUmwVqG049CswUk1Fh4HWgDbckByLH00z/46ytJJ0sBuUggkUuUnvtsbsk8Swb4+Km9wpIfZfXU2EV0tf/Z7zhTsBzVTCTT78m5
EqZKm1GHT9VTIX7Vii90xUQI6KwQeZpJWW/JAee64HvCL0iDPyTu86r+mAwDP+esFTmYtlxPVJMjORkR5E/BGpdlxHPvxkfkPXdUpudixPKgxiUG0o7c6v0d0Mr5XF5CtMeGEDQrW+JqDGBmifJNzA
dye676/mRUUpQejidXg830CZLkIIncj07hbyLr5Nd060ajdDDs+1D4VQJmMX08/dwHoDkOU0Haoi4rHgihI5zY7L4wSnmYr7FgjmI0FFM67q4p63FFtpXN0YNwPLBg3RovdEj/nFcDNUvfVfQcvQCZU=
', 'HMAC': '0V7ZWaryFvkkv1GDj5f0iUXNn7iwnGutqhB4uBgUlpQ='}
2019-12-15 06:11:44 flavia root[7975] INFO New message: {'type': 'ERROR', 'message': 'Authentication failed'}
2019-12-15 06:11:44 flavia root[7975] WARNING Got error from server: None
2019-12-15 06:11:44 flavia root[7975] INFO New message: {'type': 'ERROR', 'message': 'See server'}
2019-12-15 06:11:44 flavia root[7975] WARNING Got error from server: None
2019-12-15 06:11:44 flavia root[7975] INFO The server closed the connection
(venv) falacio@flavia:~/Desktop/Authentication-and-Access-Controls$
```

Autenticação sem sucesso (Password errada)

Autenticação do cliente com Cartão de Cidadão

Criação e Validação da chain de certificados:

São passados os certificados pela função e caso o issuer do certificado esteja presente em self.user_roots (certificados intermédios) ou self.roots (certificados do sistema) é adicionado o certificado ao array **chains** que é calculado novamente até que o issuer do zero que diferetificado que está a ser passado seja igual ao subject do certificado.

Na validação da chain, são validados os seguintes campos: **purpose**, **common_name**, **signature**, **crl** e **datas**.

- **purpose:** é o campo no certificado que vai indicar para que é que o certificado vai ser usado. SERVER_AUTH é usado para indicar certificados que podem ser usados para TLS Web Server Authentication. Para o cliente existem duas situações, o primeiro certificado da cadeia que é o CC, tem um parâmetro no key usage que é o digital_signature (que é true quando a chave pública é utilizada para verificar assinaturas digitais), para a restante cadeia é key_cert_sign (true quando a chave pública é utilizada para verificar assinaturas)
- **common_name:** common name refere-se ao nome do issuer. Para validar o certificado, o common name do certificado que vem a seguir na cadeia tem de ser igual ao common name deste..

- **signature:** é um campo de cada certificado que é criado com a chave privada do seu issuer (o que o signature faz é pegar na chave do issuer e validar)
- **crl:** lista de certificados revogados e para cada certificado da cadeia é verificado se não está nessa lista
- **datas:** é verificado se o certificado está expirado baseando-se no seus métodos **not valid before** e **not valid after**. Se o tempo atual estiver entre os valores retornados por estes métodos, o certificado é válido.

A diferença entre a validação da chain dos certificados do cartão de cidadão e dos certificados do servidor (autenticação do servidor através de X.509), é a validação do purpose, que utiliza métodos diferentes.

O desafio mecanismo resposta para a autenticação com cartão de cidadão inicia-se com o envio de uma mensagem do cliente com um pedido de challenge onde adiciona o **certificado CA do CC**. Após isto, o server guarda o certificado que foi enviado e vai validar a cadeia de certificados do certificado enviado. Se falhar a validação, encerra a conexão, se conseguir validar, envia para o cliente um nonce; ao receber este nonce, o cliente assina o nonce com a **chave privada do cartão de cidadão** e envia-o para o servidor.

O servidor, ao receber o nonce assinado, vai assinar o nonce que enviou anteriormente com a **chave pública do cartão de cidadão** (que extrai do certificado que lhe foi enviado anteriormente) e compara com o que recebeu. Se a comparação for válida a troca de mensagens prossegue, caso contrário, a conexão é terminada.

```
2019-12-15 06:55:48 flavia root[9141] INFO Sending challenge
2019-12-15 06:55:48 flavia root[9141] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'rlasRyVpWEkIakFIz69wGqmAb/zvUEAE+Z90KowUgHkQpkUaSzvTRUJEKcp5J7
GDsNvKU51b4dJ580Yb0BHLQMsVlatnigUvvyqNnXIypZZUKWDGKY69KQ==', 'HMAC': 'Axtfh0JyNyvkMYSixXllig=='}
2019-12-15 06:55:52 flavia root[9141] INFO New message: {'type': 'CHALLENGE_RESPONSE_CC', 'nonce': 'UXupghWxp8LOHcT65EwFzq3IG5DPL4v529ozUAuhAZvLBwcZpd
wXpu1m/XF1JiEYyp05T9ysr/Bz7SZAxrDV20vr4N/PFWgI8+65jLdTirU5sUxzhn7Kqu4nUExlia9ytlJAx+ykDeBIzbdIfJmcYnqu5eJGY8C+YoP7dBZSA0vI/jwH5euEPTznfK4RzgZTMz5EBcXF
FX62CDhQzW0TQeZC4XergvYBox1Un7Ua5Ru64RrTiS90HCOo4Nt0fAukYWrNdjLul68CfDTYOY0HEpniFmcup4WWuP9visakRL5g89IvSsZC6CCDsXoex5C8YPsCkf+6e0P1x9EqG0Tzw=='}
2019-12-15 06:55:52 flavia root[9141] INFO Send: {'type': 'AUTHENTICATION_OK'}
2019-12-15 06:55:52 flavia root[9141] INFO user authenticated
```

User autenticado com CC

Mecanismo Controlo de Acesso

Na criação dos users exemplo criámos 1 de cada tipo, user com permissões para descarregar o file e outro sem permissões.

O controlo de acesso foi feito com "flags", ao verificar a autenticação do username + password verifica também se este tem permissões, caso tenha prossegue para a transferência do ficheiro, caso não tenha, cancela a transferência e termina a sessão.

```
2019-12-15 05:13:59 flavia root[5800] INFO Got nonce, going to respond to challenge
Use user, pwd (flavia, flavia) to try a user that its allowed to get the files
Use user, pwd (tomas, tomas) to try a user that its NOT allowed to get the files
Username: tomas
Password:
2019-12-15 05:14:02 flavia root[5800] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'eRAhKF0DIRYfX9gEPIT3EIF0jCL2usJ276TxSCHqV4cPE1+v8Yput1KK6c7YnJ
dh2rHVBjgTCydfwYKNZYXyIj7YIDLvlgYLFGBIA910cY//fg2qVdXWliXraTyeQLQbMOW0T0/YtZpQ2nkWGFqKzTqArB/d9e0Mdwk3S2rm60asuyogG2BFIL9b+HIK7C92cwR4rOW1UdQhLEn1/9N
rYEPcWTxGrfA9d6yEsq4DS06Ai4wmqkoSlo/LJ35xbx50gqsnnl8bLMG3cV0dRLLfyKfDoHASa6SBICA3Lz4rMo6TDlnthuMxgCpP78TJ7pP9wKI8tSy/mMwCw/WGBcTLPdaPaoJrcbLZF02tXbyKDb
uhC1WsmOSxdKYwgInt9hYRg7pgt0Fr7N61KWfprT7ZyRjLEhezIaGLBKcTozXKRv5K7vbrm4AVKJTD7X2pbghUGEDrJVwXXGt6ZaIVrb9Zph17VAV+p5UzvunZP1giwUGCJxIRhMFZGBL72PrqZuK7
Bxa+8+uJrhZK6UtwfGx27DjBTg5XDYubohUt7t8IJ5YvvVa2wpzHP65/hR+ccJ9Tf06qEajudLMRShlQIQnVxjJhTdj94IilQQAfAdkttS4S0L5bEKq/dHWIXVg3KaF6XZ+T3dsUjMqCyuu0BE0gPc
YXvBaWR10ibYbd9lloLok/gt4IgONjgVd187hKbWdKwk1RqQEV04ovqVY62Awzf5vWjSTqbiudqp00ltY84SGBIj7M3EKThjd2sE0Rnr', 'HMAC': 'dl7ROfBrLnys0Hg5R6dQ4A=='}
2019-12-15 05:14:02 flavia root[5800] INFO New message: {'type': 'ERROR', 'message': 'User not authorized'}
2019-12-15 05:14:02 flavia root[5800] WARNING Got error from server: None
2019-12-15 05:14:02 flavia root[5800] INFO New message: {'type': 'ERROR', 'message': 'See server'}
2019-12-15 05:14:02 flavia root[5800] WARNING Got error from server: None
2019-12-15 05:14:02 flavia root[5800] INFO The server closed the connection
(venv) falacio@flavia:~/Desktop/Authentication-and-Access-Contro$
```

Utilizador NÃO autorizado a transferir ficheiro

```
2019-12-15 05:13:09 flavia root[5723] INFO New message: {'type': 'CHALLENGE_PASSWORD', 'nonce': 'edp3XjCoR9aFNURDLiG5KA=='}
2019-12-15 05:13:09 flavia root[5723] INFO Got nonce, going to respond to challenge
Use user, pwd (flavia, flavia) to try a user that its allowed to get the files
Use user, pwd (tomas, tomas) to try a user that its NOT allowed to get the files
Username: flavia
Password:
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciDABE1Y/G8hdeMBC9+E00F47ng23J+Nj+Ykupt2rHp273AsDg9rCB
g9uGdczkLbpvJPSl3VcwMuXMNq9KhXOuXdpMpf8mF4MbZjKXdy4q0+yGIFX530i/Ve02iW1HymGebU07LZwu+yNaYJdT+J07JXBD4RTL232FTk62808ep0XXnmGdORIG4E91PBqBwGVgphByx7I7n
xv4Iesim8vptxKJCSDTCPEPBjT1p89VeXPcw8o45lnlP0gIRw22lsJHgAuZmNqpKwnN+xQms933L1NZ05d1b6ROGaQ8CKVPZ0YnaedArsesAA/q5o/Ln+JSM5mAZPLRC7Mp71GtsPrhgJw1KIX9kL
xGn2wJVLHc+sZtsrEy5JmQyeYL7abD/xo804pVRaQA593M3mk0ZktFLLNHJ7ZztWp1VWIR432eD3P/A0jy6AY4JXAZI3r8mSChyzYkkl7JxTDLPLjtizw10vVnXsKAWeyeb3TFQu0YV2kcKUWgk0
RCZDJ4JHIqZLPbw1+3MMumfyxtmxmLWycycTNZ8gLWZHyi8oFGJ84ongSVZ6ggcySta92bryDUQgcBwxMP/IqckJgKe5PF0FXRC5FK6pp0IKgLEKfFvNWB4BR5F5VMVINRxx7U0rD3biNa3wu6/Ql/
3+03N929AIFnNh9RnFGLDP/Y8pLU0vKdF21t+L4eT29YtwqKzboBckJZOmA3MaI8IG09/OVNlOaZx3gYtQ8XtUXNIQUtNow==', 'HMAC': 'HCjbdWYCB03fQKVM++AF1g=='}
2019-12-15 05:13:13 flavia root[5723] INFO New message: {'type': 'AUTHENTICATION_OK'}
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciDd+XNY+kkW2kCS56CyP/A/V0ZhTrCigno0X71JU++3L/J3eV3emH
X+IehyqklJ/W5yF41TYSw6MA2Kuv6BjMiLjZzFif87XBSQ5UwIlr4E1WYWGXSmwCf3JXkJwG60i6e0K0kAqIxqMOBYtuwaqRw/yOD0bq4U2sT+o7T4Kp5UQthbkUTYzjK', 'HMAC': '6AVg2sEp
48KetrXfclnLEw=='}
2019-12-15 05:13:13 flavia root[5723] INFO New message: {'type': 'OK'}
2019-12-15 05:13:13 flavia root[5723] INFO Channel open
2019-12-15 05:13:13 flavia root[5723] INFO Sending file: /home/falacio/Desktop/Authentication-and-Access-Contro/requirements.txt
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciC02dwB/BNVbbTvzsZyHh3j7VmKACivURKUEcWVvIr2wNSJUAGB5
RVfKTLljgFD1pA/NYnJOGWgYNQ4ByDddXPu0Gr6VDSe+h2f9blT22cBIsoopf561eoE7rJdYwcKBXTUmp2HFDR3usNKejiTAug8Ugb6Fzy5uIR10ryFLyV6hg0QstEgUdmZRHmhaVqJ/Z9Yk5tFN
l9Pe3rZNAcSpBsqV/0TFMB8=', 'HMAC': 'EPgELjEwL06GkasC+0x0Ug=='}
2019-12-15 05:13:13 flavia root[5723] INFO Send: {'type': 'SECURE_MESSAGE', 'payload': 'x8q9vrL4ciCKN7HAoFMDNsEBTLlpsm8GkxwwQShM/vA=', 'HMAC': 'LherGH
FnrC8jHYGfeq8KXg=='}
2019-12-15 05:13:13 flavia root[5723] INFO File transferred. Closing transport
2019-12-15 05:13:13 flavia root[5723] INFO The server closed the connection
(venv) falacio@flavia:~/Desktop/Authentication-and-Access-Contro$
```

Utilizador autorizado a transferir ficheiro

Mecanismos de Segurança Adicionais

Como mecanismo de segurança adicional acrescentamos uma pergunta de verificação do utilizador. Cada utilizador tem a sua resposta. Do estilo de perguntas de segurança como “qual o nome do seu primo mais velho”, etc.

```
2019-12-15 05:26:54 flavia root[6352] INFO New message: {'type': 'CHALLENGE_PASSWORD', 'nonce': 'e+Vsf1y4XistM1GjPpsPJQ='}
2019-12-15 05:26:54 flavia root[6352] INFO Got nonce, going to respond to challenge
Use user, pwd, secret (flavia, flavia, galinha) to try a user that its allowed to get the files
Use user, pwd, secret (tomas, tomas, ovo) to try a user that its NOT allowed to get the files
Username: tomas
Password:
Qual e coisa qual e ela...: galinha
```

Questão segurança ao utilizador

Caso a resposta à questão secreta não esteja correta a sessão é terminada. Se estiver correta, a autenticação é efetuada (caso tenha permissões).

Conclusão

A realização do nosso protocolo foi, a nossa ver, realizada com sucesso, uma vez que a comunicação entre o servidor e o cliente está estruturada de maneira bastante segura e robusta e o controlo de acessos dos clientes está a funcionar na plenitude. Foram implementados todos os tópicos que nos foram propostos: Autenticação do Servidor, Autenticação do Cliente através de CC e Password, Mecanismos de desafio resposta e Mecanismos de defesa adicionais.

O tópico onde tivemos mais dificuldades foi a autenticação através de CC.

Todas as validações estão a ser corretas e exatas e sem quaisquer problemas.

Em suma, apesar dos problemas enfrentados durante o desenvolvimento, concluímos que o balanço foi positivo, resultando assim num protocolo robusto e funcional para vários tipos de autenticação.

Bibliografia

- Consulta de vários temas da documentação do Cryptography IO