Capítulo 6 – Protocolos de Autenticação

A autenticação de entidades consiste na obtenção de um comprovativo de que elas possuem um atributo que afirmam possuir, ou que é suposto que possuam.
A autenticação de entidades envolve um processo de prova, na qual o autenticador obtém uma prova fidedigna de que a entidade autenticada, ou autenticado, possui o atributo que afirma possuir.
Um **protocolo de autenticação** é um conjunto de mensagens trocadas entre vários interlocutores, e que tem por objetivo realizar a autenticação de um ou mais deles perante um ou mais dos demais.

6.1. Caracterização dos protocolos de autenticação

6.1.1. Elemento de prova

São usados três tipos de paradigmas em termos de elementos de prova:

- *O que sabe*: uma entidade prova a sua autenticidade mostrando que conhece uma determinada informação secreta, denominada genericamente por senha. Se a senha for conhecida pelos intervenientes diretos no processo de autenticação, pode provar que o interlocutor é quem afirma ser.
- *O que possui*: Neste paradigma uma entidade prova a sua autenticidade mostrando que possui um determinado dispositivo de segurança ou que é o dono legítimo desse dispositivo de segurança.
- *O que se é*: Neste paradigma é apresentado alguma característica que a permite diferenciar das demais. Normalmente este paradigma aplica-se a humanos e a característica diferenciadora é obtida através da biometria.

Quando se usam estes três paradigmas combinados diz-se que a sua autenticação é **multimétodo**.

6.2. Autenticação: Objetivos

- Autenticar entidades interatuantes
    - pessoas, serviços, servidores, máquinas, redes, etc
- Permitir aplicação de políticas e mecanismos de autorização
  Autorização → autenticação
- Apoiar outras ações no âmbito da segurança
    - distribuição de chaves para comunicação segura

6.3. Autenticação: Requisitos

- **Confiança**
  Nível de confiança
- **Secretismo**
  Não divulgação de credenciais usadas pelas entidades legítimas
- **Robustez**
  Impedir ataques às trocas de dados do protocolo;
  Impedir cenários de DoS interativos
  Impedir ataques desligados com dicionários

- Simplicidade

Deverá ser tão simples quanto possível para evitar que os utentes escolham simplificações perigosas

- Lidar com vulnerabilidades vindas das pessoas

Têm uma tendência natural para facilitar ou para tomarem iniciativas perigosas

6.4. Autenticação: Entidades e modelos de implantação

Entidades	Modelos de implantação
Pessoa Máquinas Redes Serviços/servidores	- Ao longo do tempo -- quando a interação se inicia -- continuamente ao longo a interação - Direccionalidade -- Unidirecional -- Bidirecional

6.5. Protocolos de Autenticação: Aproximações Elementares

- Aproximação Direta

Apresentar credenciais

Esperar pelo veredicto

- Aproximação com desafio-resposta

Na apresentação da prova de autenticação existem dois paradigmas: explícita e implícita.

Explicita	Implícita
O autenticado apresenta explicitamente o seu elemento de prova ao autenticador	O autenticado mostra ao autenticador que sabe ou possui o elemento de prova, mas nunca o apresenta explicitamente

Desafio-Resposta com funções invertíveis
O autenticador aplica à resposta uma operação inversa à usada. Este tipo de diálogo pode ser concretizado com funções de cifra simétrica (Figura 1), com base numa chave secreta partilhada *k*, ou assimétricas com ase num par de chaves privada/pública (Figura 2). Em termos de segurança, a ideal é esta última, porque não implica a partilha de um segredo entre as partes: o autenticador apenas precisa de conhecer a chave pública do autenticado.

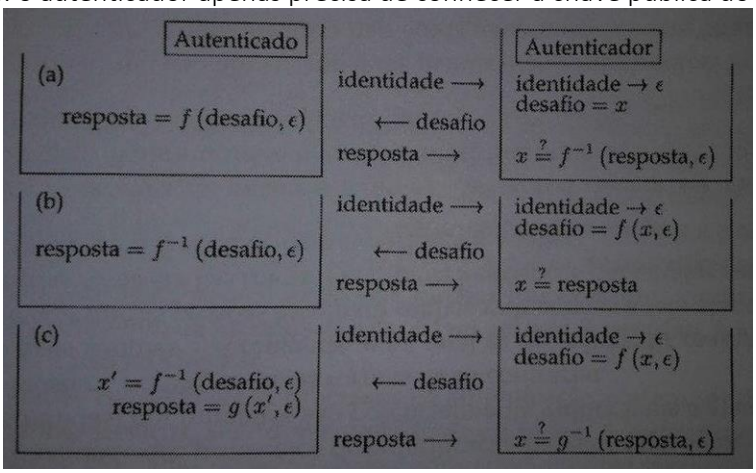


Figura 1

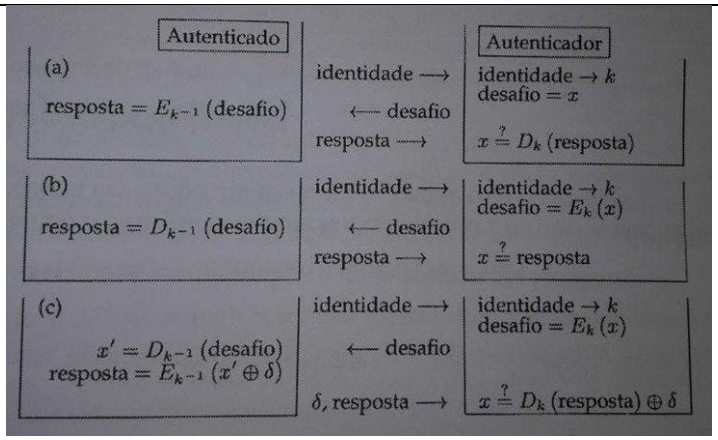


Figura 2

Desafio-resposta com funções não invertíveis

No caso das funções de transformação não invertíveis ambos aplicam a mesma função ao desafio para obter a resposta e o autenticador verifica se a resposta recebida é igual à que ele mesmo calculou (Figura 3). Neste caso volta a ser necessário que o autenticador partilhe com o autenticado um elemento e prova, ou seja, um valor secreto *k*. No entanto, a função de transformação pode ser uma qualquer função não invertível, sendo tipicamente usada uma função de síntese ou alguma função similar (Figura 4).

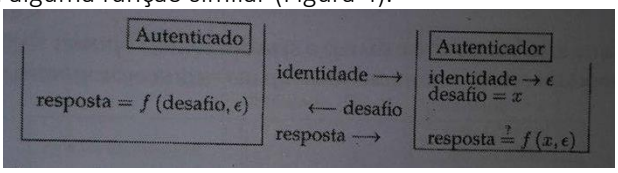


Figura 3

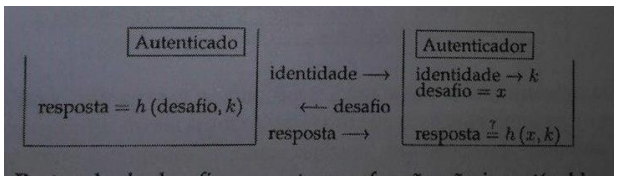


Figura 4

6.6. Autenticação de pessoas: Aproximação direta com senha memorizada

Os protocolos de autenticação com segredo partilhado são os mais simples que existem. Estes protocolos permitem a autenticação com apresentação explícita ou implícita de credenciais e a autenticação mútua.

O método clássico de autenticação de utentes (pessoas) em sistemas operativos é através de pares constituídos por um nome de utente (*username*) e uma senha (*password ou passphrase*). O sistema autenticador guarda estes pares e confirma, para um determinado par, se ele existe. Se existir, a autenticação do titular do par foi corretamente efetuada. Se não existir, o utente existe ou enganou-se na sua senha.

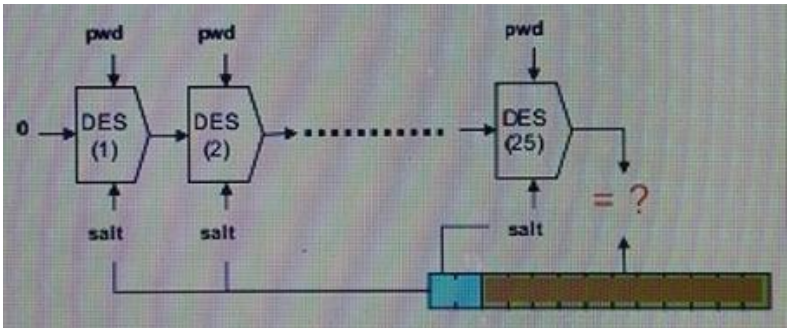
As senhas não são guardadas inalteradas nos sistemas operativos, pois tal poderia facilitar a sua observação em caso de falha dos mecanismos de proteção do suporte de armazenamento. Para resolver esses problemas, as senhas são guardadas transformadas através de uma função unidirecional. As senhas introduzidas pelos utentes são transformadas por essa mesma função antes de serem comparadas com as senhas guardadas.

As senhas são transformadas usando um valor aleatório, comummente designado por sal (*salt*). Este sal é escolhido quando se realiza a primeira transformação da senha e depois é armazenado para usos futuros dessa mesma senha:

sal | senha transformada = *f*(sal,senha)

onde o operador | representa concatenação.

O objetivo primordial do sal é o de evitar que a mesma senha, usada pelo mesmo utente ou por utentes diferentes no mesmo ou em vários sistemas, para produzir transformações iguais.



- Vantagens

Simplicidade

- Problemas

Utilização de senhas fracas/inseguras que permitem ataques com dicionários

Transmissão de senhas em claro em canais de comunicação inseguros como escutas que podem revelar senhas, como por exemplo serviços remotos do UNIX, PAP

6.7. Autenticação de pessoas: Aproximação direta com Biometria

A autenticação biométrica baseia-se na avaliação de características físicas dos autenticadores para aferir a sua autenticidade face a uma identidade reclamada. Essas características podem ser diversas, e tanto fisiológicas e estáticas (dimensões e distancias faciais) como comportamentais e dinâmicas (ritmo de escrita num teclado).

- Uma pessoa autentica-se usando medidas do seu corpo

Avaliações biométricas

Impressão digital, iris, geometria da face timbre vocal, escrita manual, etc.

- Estas medidas são comparadas com um registo pessoal similar

Referências biométrica

Criado no sistema de forma similar mas no âmbito de uma inscrição anterior

- Vantagens

As pessoas não precisam de memorizar nada só precisam de ser elas mesmo

As pessoas não podem escolher senhas fracas de facto, não escolhem nada

As credenciais não podem ser transferidas entre pessoas, não é possível delegar a autenticação própria.

- Problemas

A biométrica ainda está incipiente. Em muitos casos pode ser enganada facilmente.

As pessoas não podem mudar de credenciais, caso estas sejam roubadas.

As credenciais não podem ser transferidas entre pessoas. Caso seja necessário em situações excecionais.

Pode criar riscos para as pessoas. Remoção de partes do corpo para personificação da vítima.

Não é fácil efetuar autenticação remota. É preciso confiar na infraestrutura remota de aquisição de dados biométricos.

A biometria pode revelar informação pessoal sensível. Doenças.

6.7. Autenticação de pessoas: Aproximação direta com senhas descartáveis

A autenticação com senhas descartáveis é um tipo de autenticação com apresentação direta de credenciais onde as mesmas nunca se repetem, só são usadas uma vez. Este tipo de autenticação é interessante quando se pretende riscos que o mesmo apresenta quando as credenciais podem ser capturadas por terceiras e reutilizadas posteriormente. Com as senhas descartáveis a captura não é evitada, mas o risco da mesma é eliminado porque uma senha descartável não é reutilizável.
Exemplo de senhas descartáveis: matriz com códigos bancários.

Vantagens
- Podem ser escutadas, isso não adianta a quem o fizer para personificar o dono da senha.
Problemas
- As entidades interatuantes precisam de saber que senhas devem usar em diferentes ocasiões, o que implica uma qualquer forma de sincronização. - As pessoas podem precisar de recursos extra para manter ou gerar senhas descartáveis, como: folha de papel, programa de computador, dispositivos adicionais, etc. - Cria uma sobrecarga ao autenticado, que deverá possuir e usar um método para calcular a senha descartável enviada em cada autenticação. Deverá haver uma correta sincronização entre o autenticado e o autenticador, de forma a que a senha descartável enviada pelo primeiro seja a esperada pelo segundo.

O sistema RSA SecurID, usa a contagem do tempo como elemento de sincronização entre o autenticador e o autenticado. O autenticado dispõe de um equipamento próprio com um relógio que, está sincronizado como o relógio do autenticador. Os minutos contados por ambos os relógios são usados no processo de cálculo da senha descartável. A ocorrência de dessincronizações entre os relógios, devido a tolerâncias de erro no fabrico dos cristais dos relógios, levam a que o autenticador tenha de incluir funcionalidades extra para lidar com essa realidade.

Caso de Estudo: RSA SecurID

O RSA SecurID é um sistema de autenticação com senhas descartáveis que usa chaves secretas, partilhadas entre autenticador e autenticado. O autenticado guarda a chave num equipamento próprio, que a usa para produzir senhas descartáveis num ritmo fixo.
A autenticação com RSA SecurID faz-se usando uma técnica de autenticação multimétodo dupla: um PIN e a senha descartável. O PIN deve ser memorizado (algo que se sabe) e a senha descartável é gerada pelo equipamento (algo que se tem). A senha descartável é calculada usando dois parâmetros: a chave secreta partilhada e o instante temporal em que a geração se

faz. O objetivo do PIN é o de impedir que alguém que roube um dispositivo RSA SecurID e conheça a identidade de acesso do seu dono, o consiga personificar.

O número único é calculado com base numa chave de 64 bits guardada no equipamento, a data/hora atual, um algoritmo exclusivo (SecurID hash) e um PIN extra (apenas para alguns equipamentos).

Uma pessoa gera uma OTP (one-time password) combinando o seu User ID com o número apresentado pelo equipamento.

OTP = UserID, Token Number

Um RSA ACE Server faz o mesmo, dado o User ID e verifica a igualdade, pois também conhece a chave pessoa guardada no equipamento. Tem de haver alguma sincronização extra para lidar com desvios dos relógios. (RSA Security Time Synchronization).
Robusta contra ataques com dicionários, pois as chaves não são escolhidas por pessoas.

6.8. Aproximação com desafio-resposta: Descrição genérica

O autenticador fornece um desafio. A entidade a ser autenticada transforma o desafio usando as suas credenciais de autenticação. O resultado é enviado para o autenticador.

O autenticador verifica o resultado, onde produz um resultado próprio usando a mesma aproximação e verifica a igualdade e produz o valor a partir do resultado e verifica se iguala o desafio ou algum valor relacionado.

Vantagens
- As credenciais de autenticação não são expostas.
Problemas
- As pessoas tem de ter meios para calcular respostas a partir de desafios, como hardware ou software. - O autenticador poderá ter de manter segredos partilhados. - Ataques com dicionários autónomos usando pares desafios-resposta, onde se consegue revelar o segredo usado para calcular a resposta.

6.9. Autenticação de pessoas: Desafio-resposta com smartcards

Credencias de autenticação com o smartcard (Cartão de Cidadão), a chave privada guardada no smartcard e o pin de acesso à chave privada.
O autenticador sabe a chave pública correspondente.

6.9.1. Protocolo com desafio-resposta

O autenticador gera um desafio aleatório ou um valor nunca antes usado. O dono do smartcard cifra o desafio com a sua chave privada, guardada no smartcard e protegida pelo PIN.

O autenticador decifra o resultado com a chave pública se o resultado for igual ao desafio, a autenticação teve sucesso.

6.10. Autenticação de pessoas: Desafio-resposta com senha memorizada

As credencias de autenticação é a senha selecionada pelo utente. O autenticador sabe a transformação da senha e esta é preferencialmente unidirecional.

6.10.1. Protocolo com desafio-resposta elementar

O autenticador gera um desafio aleatório ou nunca antes estudado. O utente calcula uma transformação do desafio e da senha, como por exemplo: uma síntese comum onde a

Resposta = síntese(desafio,senha)

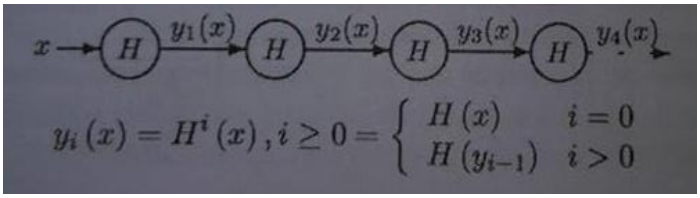
O autenticador faz o mesmo ou inverso se os resultados forem iguais, a autenticação teve sucesso.

Exemplo YubiKey:

- Equipamento de autenticação pessoal (USB ouNFC)
- Geram uma chave única de cada vez
    - associado a uma pessoa
    - Emula um teclado USB
    - Implementa HMAC-OTP (HOTP)
    - Robusta contra ataques com dicionários (as chaves não são escolhidas por pessoas)
- Pode armazenar dados confidenciais:
    - Logins e passwords
    - Bloqueados num "cofre" até serem pedidos por um utilizador autenticado
- Pode conter um par de chaves RSA 2048
    - Implementa protocolo OpenPGP card
    - Permite acesso contacless (via NFC)
    - Realiza operações de assinatura sem expor chave privada

Caso de Estudo: S/Key e OTP

O S/Key e o OTP são dois protocolos que se baseia numa cadeia de dispersão (hash chain).
Uma cadeia de dispersão consiste na aplicação sistemática de uma função de dispersão ao resultado da operação anterior.



O processo idealizado consiste em que o autenticado memorize uma senha e um índice, calcula o valor de $y_{indice}(senha)$ e entrega ao autenticador esse valor como elemento de verificação da sua autenticidade.

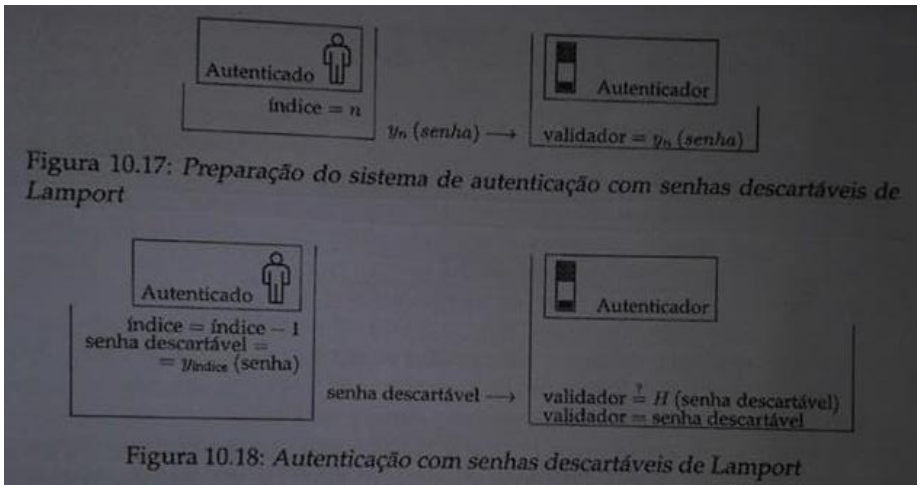


Figura 10.17: *Preparação do sistema de autenticação com senhas descartáveis de Lamport*

Figura 10.18: *Autenticação com senhas descartáveis de Lamport*

Caso de Estudo: PAP e CHAP

- Protocolos usados com PPP (Point-to-Point Protocol)
    - Autenticação unidirecional, pois o autenticador não se autentica ou não é autenticado.
- PAP (PPP Authentication Protocol)
    - Apresentação simples de um par UID/senha
    - Transmissão (insegura) da senha em claro
- CHAP (CHallenge-response Authentication Protocol)

    Aut → U : authID, desafio

    U → Aut: authID, MD5(authID, senha, desafio), identidade

    Aut → U : authID, OK/not OK

    - O autenticador pode requerer a autenticação em qualquer instante.

6.11. Autenticação de pessoas: Desafio-resposta com chave partilhada

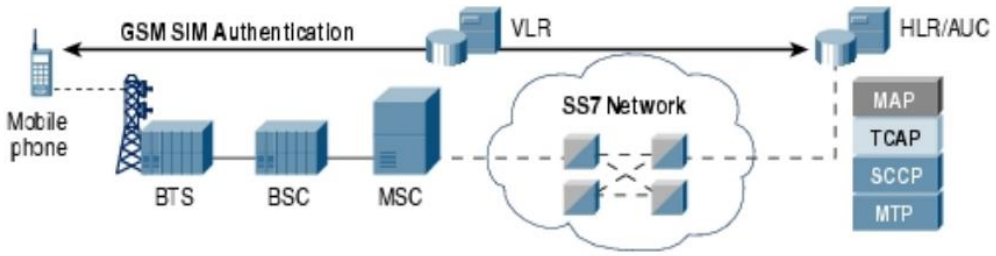
Uma solução para problemas com ataques consiste na substituição de uma senha memorizável por uma chave secreta, guardada de uma qualquer forma mas não memorizada. O facto de não ter de ser memorizável tem como vantagem o facto de não precisar de ser escolhida pelos utentes, podendo ser gerada aleatoriamente.

Assim, usa uma chave criptográfica partilhada em vez de uma senha o que torna mais robusto contra ataques de dicionário e requer um dispositivo para guardar a chave.

Caso de Estudo: GSM

Nas redes "celulares" GSM cada cliente, designado por subscritor, possui um smartcard com um módulo SIM (Subscriber Identification Module). Um módulo SIM é uma componente da arquitetura de autenticação do GSM que é responsável pelo armazenamento, proteção e exploração de uma chave secreta de autenticação do subscritor titular. Na prática os módulos SIM são concretizados por smartcards de reduzida dimensão que são colocados no interior dos telefones.

O processo de autenticação consiste num protocolo desafio-resposta com chave secreta partilhada.



Baseada numa chave secreta partilhada entre o HLR e o telefone móvel
- 128bits Ki, guardada no cartão SIM do telefone móvel
- Só pode ser usada após a introdução do PIN de desbloqueio

Algoritmos (inicialmente não públicos):
- A3 para autenticação
- A8 para gerar a chave de sessão
- A5 para cifrar a comunicação

A3 e A8 realizados pelo cartão SIM
- Podem ser escolhidos pelo operador

6.12. Autenticação de Máquinas

A autenticação de máquinas pode ser efetuada por nome ou endereço ou com chaves criptográficas.

Por nome ou endereço: nome DNS, endereço IP, endereço MAC, entre outros. É extremamente fraco pois não existe prova criptográfica.

Com chaves criptográficas: as chaves secretas são partilhadas com interlocutores usuais. Pares de chaves assimétricas por máquina, onde chaves públicas são pré-partilhadas com interlocutores e chaves publicas certificadas por terceiros.

6.13. Autenticação de Serviços/Servidores

A autenticação da máquina hospedeira diz que: todos os serviços co-localizados são automaticamente e indiretamente autenticados. Existem credenciais próprias do serviço.

A autenticação é feita por chaves secretas partilhadas com clientes quando evolvem a autenticação dos clientes com as mesmas e com pares de chaves assimétricas por máquina/serviço, certificadas por terceiros ou não.

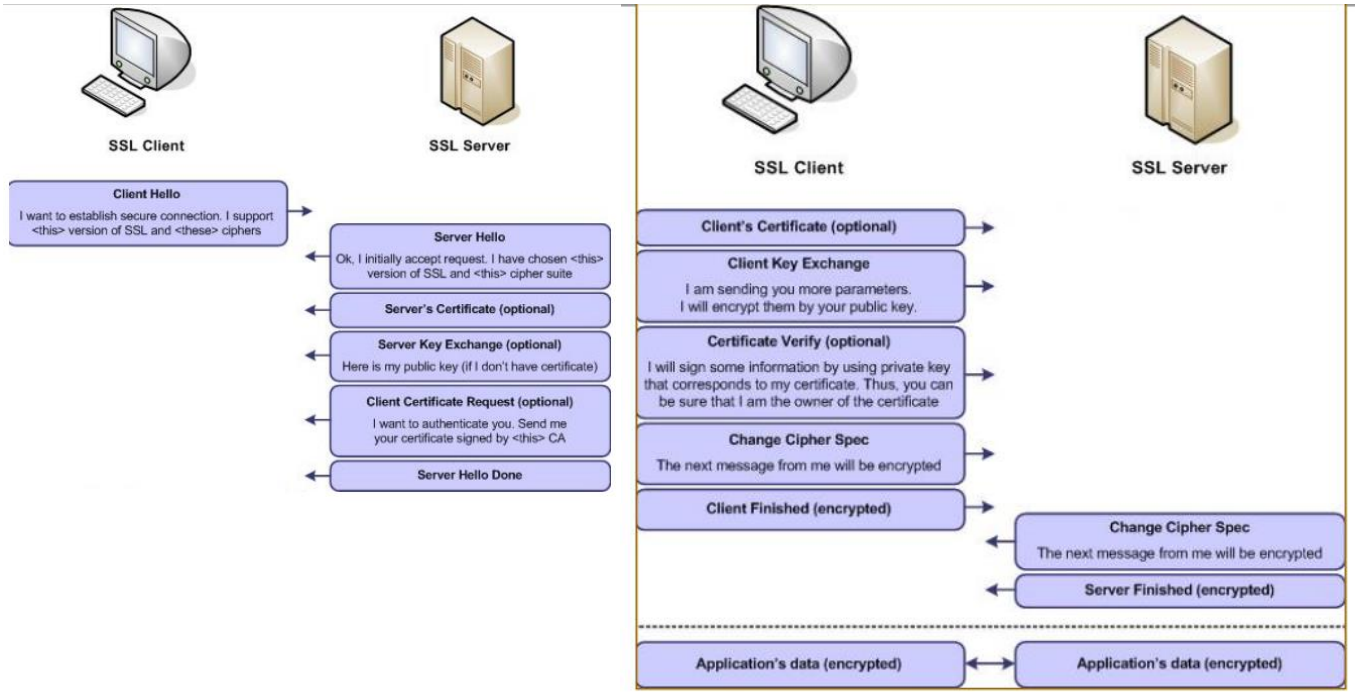
Caso de Estudo: SSL/TLS

O SSL/TLS assegura uma comunicação segura cliente-servidor sobre transportes com ligação, nomeadamente TCP/IP. Para o efeito, cliente e servidor negoceiam os parâmetros de uma sessão segura. Nessa mesma negociação ambos os negociadores, podem-se autenticar usando pares de chaves assimétricas e certificados X.509 da respetiva chave publica. A autenticação do cliente implica uma autenticação mútua, mas o inverso não.

A autenticação do cliente faz-se de maneira diferente da autenticação do servidor. A do servidor valida o certificado apresentado na mensagem *Server Certificate* e confirma.se se o mesmo pertence ao serviço desejado e usa-se a chave pública do servidor para lhe enviar uma chave de sessão de forma secreta e autenticada na mensagem *Client Key Exchange*.

No caso do cliente este autentica-se explicitamente realizando uma assinatura com a sua chave privada. Essa assinatura é enviada na mensagem *Certifcate Verify* e é realizada sobre todas as mensagens trocadas no protocolo até esse momento.

A autenticação do cliente não é decidida voluntariamente, é imposta pela inclusão da mensagem *Certificate Request*. A validação do certificado do cliente implica que o servidor conheça a cadeia de certificação desse certificado.
As mensagens *Server Certificate* e *Client Certificate* possuem o certificado de chave pública da entidade que se autentica e também, uma cadeia de certificação desse certificado. Essa cadeia facilita a tarefa do validador do certificado, porque não precisa de possuir em avanço, ou procurar dinamicamente, os certificados intermédios necessários à validação do certificado do interlocutor.



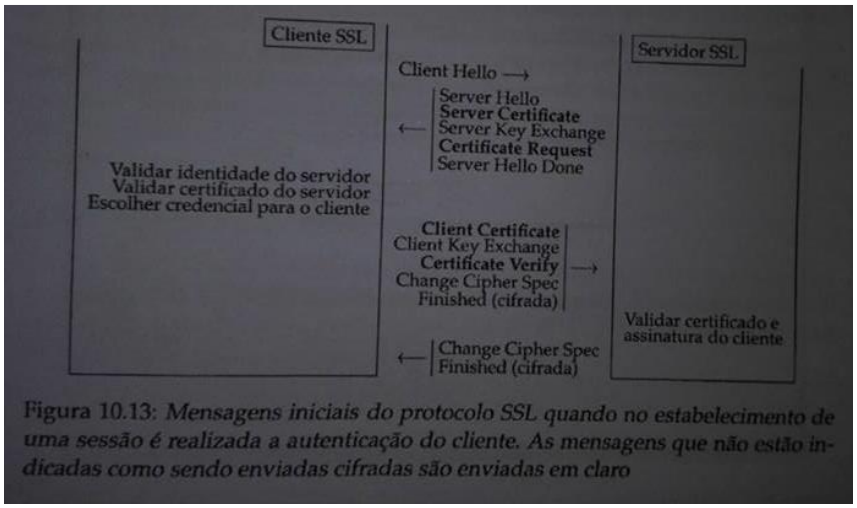


Figura 10.13: *Mensagens iniciais do protocolo SSL quando no estabelecimento de uma sessão é realizada a autenticação do cliente. As mensagens que não estão indicadas como sendo enviadas cifradas são enviadas em claro*

Mecanismos de segurança:
- Confidencialidade e integridade da comunicação na distribuição de chaves
- Autenticidade de interlocutores: servidores ou utilizadores cliente. Ambas realizadas com chaves assimétricas e certificados X.509

Caso de Estudo: SSH

O SSH permite duas formas de autenticar oc clientes: usando senhas partilhadas e usando pares de chaves assimétricas.

A primeira consiste numa exploração direta de métodos de autenticação nativos do sistema operativo do autenticador, baseados em processos elementares de apresentação direta da senha pelo cliente. No caso SSH esta apresentação da senha não tem riscos de segurança porque a senha circula entre cliente e servidor dentro do canal de comunicação seguro e criado previamente pelo SSH.

A segunda, usando o par de chaves assimétricas para autenticar o cliente, o mesmo apenas precisa, no máximo, de saber uma senha: a que protege a sua chave privada. Se essa senha for comprometida é apenas necessário troca-la num único local: no sistema onde a chave privada está guardada. A aplicação cliente SSH, onde quer que seja usada por esse cliente, terá de ser configurada para usar a sua chave privada a partir do local onde a mesma está guardada.

Estes pares de chaves assimétricos podem ser gerados por aplicações próprias apenas para serem usados pelo SSH, mas é igualmente possível usar outros pares de chaves assimétricas geradas para outros fins.

A aplicação cliente baseada e adaptada para trabalhar com smartcards através da interface PKCS#11 do Cartão de Cidadão na qual se indicam quais as credenciais a usar para autenticação do utente (nomeadamente, um cartão com o rótulo “CARTAO DE CIDADAO” e umas credenciais assimétricas, cujo certificado de chave publica possui o rotulo “CITIZEN AUTHENTICATION CERTIFICATE”).

Mecanismos de segurança:

- Confidencialidade e integridade da comunicação na distribuição de chaves
- Autenticidade de interlocutores: servidores ou utilizadores cliente. Ambas realizadas com técnicas diferenciadas.