

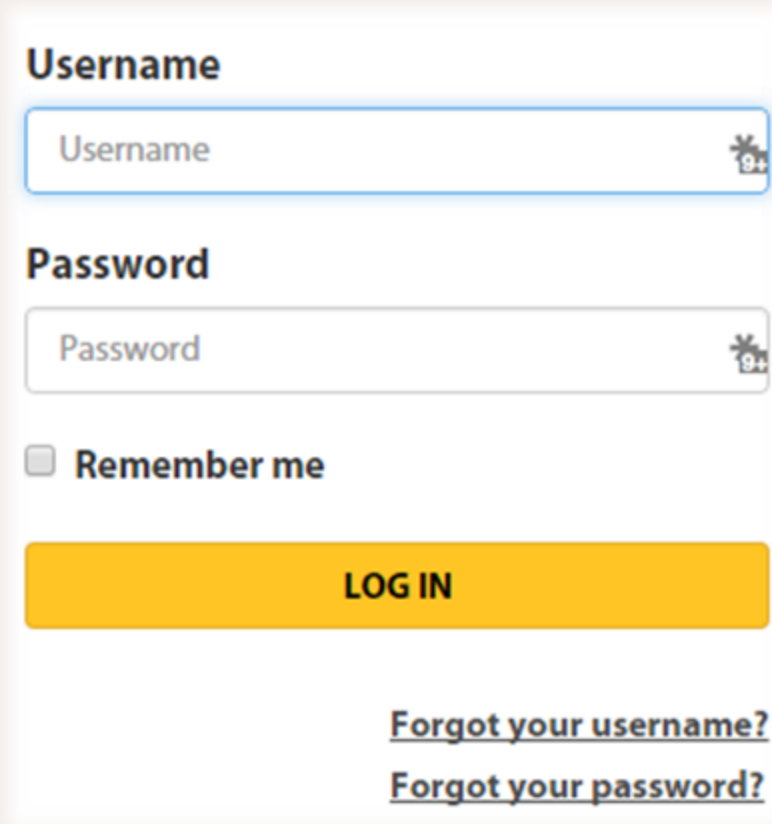
Tecnologias de Autenticação

Gonçalo Veríssimo 48738
Rúben Farinha 48329

O que são as Tecnologias de Autenticação?



Autenticação baseada em conhecimento



The image shows a typical login form. It has two input fields: 'Username' and 'Password'. Below these is a checkbox labeled 'Remember me'. A prominent yellow button labeled 'LOG IN' is positioned below the checkbox. At the bottom, there are two links: '[Forgot your username?](#)' and '[Forgot your password?](#)'. The form is set against a light gray background with a subtle shadow.

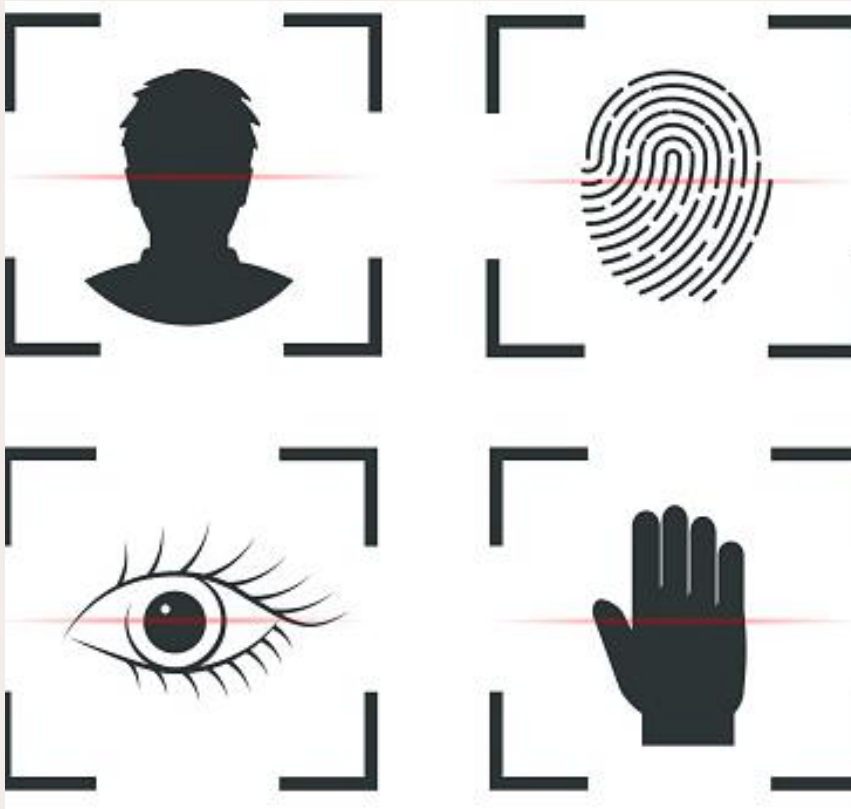
- Forma mais comum
- Baseada num segredo, apenas conhecido pelo utilizador, geralmente uma combinação "username – password"
- Simples de implementar
- Vulnerável

Autenticação por tokens

- Utiliza Tokens gerados de várias formas:
 - Físico (USB Key)
 - Autenticador
 - SMS
- Um ou vários códigos únicos gerados, com um curto espaço de "vida"
- Forte segurança



Autenticação biométrica



- Utiliza características físicas para identificação:
 - Scanner Íris
 - Reconhecimento Facial
 - Impressão Digital
 - Geometria da mão
- Conveniente e segura, porém com algum risco

Autenticação multifator

- Autenticação reforçada com várias camadas de autenticação
- Reduz significativamente acessos não autorizados
- Pode incluir variáveis combinações de acessos por:
 - Username – Password
 - Token de Segurança (SMS, Authenticator)
 - Biométrica (Reconhecimento Facial, Impressão Digital)



Chave pública e chave privada



- Par de chaves criptográficas
 - Chave pública
 - Chave privada
- Forte Segurança
- Exemplos:
 - Chave Móvel Digital
 - Acesso a servidores
 - Arquivos

Autenticação baseada em monitorização/risco

- Autenticação dinâmica e adaptável
- Controla o acesso baseado em fatores comportamentais e ambientais do indivíduo
 - Localização
 - Tipo de dispositivo
 - Comportamento
- Utilizadores de alto risco, são bloqueados temporariamente ou é pedido uma nova etapa de acesso multifator

