WHITEPAPER

MFA E 2FA: AUTENTICAÇÃO MULTIFATOR PARA ACESSO REMOTO E AMBIENTES OT

Entenda MFA e 2FA, fatores de autenticação, tokens, certificados, VPN, PAM, fornecedores, contas de emergência e aplicação em ambientes OT.

A3A® Engenharia de Sistemas

SUMÁRIO

1. O QUE É MFA 4
2. O QUE É 2FA 4
3. FATORES DE CONHECIMENTO 4
4. FATORES DE POSSE 5
5. FATORES BIOMÉTRICOS 5
6. OTP, HOTP E TOTP 5
7. TOKENS FÍSICOS OTP 5
8. PUSH AUTHENTICATION 6
9. MFA FATIGUE 6
10. SMS E CHAMADAS 6
11. FIDO2 E WEBAUTHN 7
12. PASSKEYS 7
13. SMART CARDS E CERTIFICADOS 7
14. CERTIFICADOS DE DISPOSITIVO 7
15. RESISTÊNCIA A PHISHING 7
16. MFA PARA VPN 8
17. MFA PARA PAM 8
18. STEP-UP AUTHENTICATION 8
19. MFA PARA RDP E SSH 8
20. MFA PARA APLICAÇÕES LEGADAS 9
21. MFA E RADIUS 9
22. MFA PARA FORNECEDORES 9
23. ENROLAMENTO DE FATORES 9
24. RECUPERAÇÃO DE CONTA 10
25. PERDA OU TROCA DE DISPOSITIVO 10
26. BREAK-GLASS 10
27. DISPONIBILIDADE DO SERVIÇO MFA 10
28. AUTENTICAÇÃO OFFLINE 10
29. CONDITIONAL ACCESS 11
30. DEVICE TRUST 11
31. CONTAS DE SERVIÇO 11
32. CONTAS LOCAIS 11
33. SEGURANÇA DO SERVIDOR MFA 12
34. LOGS E MONITORAMENTO 12

35. POLÍTICAS POR CRITICIDADE 12
36. EXPERIÊNCIA DO USUÁRIO 12
37. PROJETO E DOCUMENTAÇÃO 12
38. IMPLANTAÇÃO POR ETAPAS 13
39. COMISSIONAMENTO E ACEITE 13
40. DIAGNÓSTICO DE FALHAS 13
41. ERROS COMUNS 13
42. CONCLUSÃO 14

MFA é a autenticação que exige fatores de categorias diferentes para confirmar a identidade. **2FA** é um caso específico de MFA no qual dois fatores são utilizados. Em ambientes OT, MFA é aplicado principalmente a VPNs, PAM, jump servers, estações de engenharia, portais administrativos e acesso remoto de fornecedores.

A proteção não depende apenas de “pedir um código”. Métodos variam em resistência a phishing, disponibilidade, dependência de internet, sincronismo e recuperação. SMS e push simples oferecem proteção inferior a certificados, smart cards e chaves FIDO2 em muitos cenários.

MFA deve ser combinado com menor privilégio, segmentação e controle de sessão. Um usuário autenticado com dois fatores ainda não deve receber acesso amplo a toda a rede operacional.

1. O QUE É MFA

MFA significa *Multi-Factor Authentication*. A autenticação utiliza dois ou mais fatores independentes.

Os fatores clássicos são algo que o usuário sabe, possui ou é. Senha é conhecimento; token ou telefone é posse; biometria é inerência.

Duas senhas não formam MFA porque pertencem à mesma categoria. A independência entre fatores é parte do objetivo.

2. O QUE É 2FA

2FA significa autenticação de dois fatores. Toda 2FA é MFA, mas MFA pode utilizar mais de dois fatores.

No uso cotidiano, os termos são frequentemente tratados como equivalentes. Em projeto, é melhor registrar os métodos exatos.

Uma combinação pode ser senha mais TOTP, certificado mais PIN ou chave FIDO2 com verificação local.

3. FATORES DE CONHECIMENTO

Senhas e PINs pertencem à categoria de conhecimento.

Senhas precisam de comprimento, unicidade e proteção contra reutilização. O gerenciador de senhas ajuda usuários a manter credenciais distintas.

PIN de smart card ou chave não é senha do serviço; ele desbloqueia o fator de posse local. Isso pode reduzir exposição ao servidor remoto.

4. FATORES DE POSSE

Aplicativos autenticadores, tokens físicos, smart cards, certificados e chaves de segurança são fatores de posse.

O valor depende da proteção da chave e do processo de emissão. Copiar uma semente TOTP para vários dispositivos reduz controle.

Perda, substituição e revogação precisam de procedimento.

5. FATORES BIOMÉTRICOS

Biometria pode desbloquear um dispositivo ou chave local. Impressão digital e reconhecimento facial não devem ser tratados como segredo revogável.

A implementação precisa considerar taxa de erro, fallback e proteção do template.

Em muitas arquiteturas, a biometria libera uma credencial criptográfica armazenada no dispositivo, sem enviar a característica ao servidor.

6. OTP, HOTP E TOTP

OTP é uma senha de uso único. HOTP utiliza contador; TOTP utiliza tempo.

TOTP é comum em aplicativos autenticadores. Servidor e token compartilham uma semente e calculam códigos por janela temporal.

A semente precisa ser protegida. QR codes de enrolamento não devem ser armazenados sem controle.

O servidor NTP é relevante porque desvios podem causar rejeição de códigos.

7. TOKENS FÍSICOS OTP

Tokens físicos geram códigos sem depender de smartphone.

Podem ser adequados a ambientes restritos ou usuários que não utilizam dispositivo pessoal.

A logística inclui compra, inventário, associação, bateria, perda e substituição.

Tokens OTP ainda podem ser usados em phishing em tempo real, caso o usuário entregue o código a uma página falsa.

8. PUSH AUTHENTICATION

Push envia uma solicitação ao aplicativo e o usuário aprova ou rejeita.

A conveniência pode levar a MFA fatigue, na qual várias solicitações induzem aprovação indevida.

Number matching, contexto de localização e nome da aplicação melhoram a decisão. A política deve bloquear ou investigar excesso de solicitações.

9. MFA FATIGUE

Atacantes podem gerar várias notificações até o usuário aceitar.

Medidas incluem number matching, limite, detecção, treinamento e métodos resistentes a phishing.

O SIEM em ambientes OT pode correlacionar várias negações seguidas de aprovação.

10. SMS E CHAMADAS

SMS e voz são simples, mas dependem da rede telefônica e estão sujeitos a troca de SIM, interceptação e phishing.

Podem ser utilizados como transição ou recuperação, mas não são preferíveis para acessos privilegiados.

A organização deve avaliar cobertura em subestações e viagens. Ausência de sinal pode impedir manutenção.

Nem todo segundo fator oferece a mesma proteção.

SMS, TOTP, push, certificados e FIDO2 possuem resistências, dependências e procedimentos de recuperação diferentes que precisam acompanhar a criticidade do acesso.

Conhecer a solução de Zero Trust Network Access

11. FIDO2 E WEBAUTHN

FIDO2 utiliza criptografia assimétrica e vincula a autenticação ao domínio legítimo. Isso oferece resistência maior a phishing.

A chave privada permanece no autenticador. O servidor armazena a chave pública.

Chaves físicas e autenticadores de plataforma podem ser usados. A compatibilidade com VPN, PAM e aplicações precisa ser confirmada.

12. PASSKEYS

Passkeys utilizam credenciais FIDO. Podem estar vinculadas a dispositivo ou sincronizadas por provedor.

Em ambientes corporativos críticos, a política precisa definir dispositivos, backup e recuperação.

A adoção depende do suporte das aplicações e da governança de identidade.

13. SMART CARDS E CERTIFICADOS

Smart cards armazenam certificados e chaves privadas. O usuário utiliza cartão e PIN.

Eles podem autenticar estações, VPNs e aplicações. A implantação requer PKI, leitores, middleware e ciclo de vida.

Certificados podem ser adequados a equipes de engenharia, mas precisam de processo de emergência e reposição.

14. CERTIFICADOS DE DISPOSITIVO

Além da identidade do usuário, o dispositivo pode apresentar certificado.

Isso permite exigir notebook gerenciado e usuário autorizado. A combinação reduz acesso a partir de equipamentos pessoais.

Certificados precisam ser renovados e revogados. O inventário deve relacionar certificado e ativo.

15. RESISTÊNCIA A PHISHING

TOTP, SMS e push podem ser capturados ou aprovados em ataques de intermediação.

FIDO2 vincula a credencial ao domínio e reduz esse risco. Certificados também podem oferecer autenticação forte quando bem implementados.

A seleção deve considerar criticidade. Acesso ao PAM e administração de identidade merecem métodos mais resistentes.

16. MFA PARA VPN

VPN deve autenticar usuário e, quando possível, dispositivo.

Após autenticação, o usuário não deve receber rede ampla. Políticas limitam destinos e encaminham para jump server.

A DMZ entre TI e OT separa acesso remoto e ativos operacionais.

Logs de VPN e MFA precisam chegar ao SIEM.

17. MFA PARA PAM

O PAM e jump server deve exigir MFA no acesso privilegiado.

A sessão ao destino pode usar credencial custodiada sem exigir novo fator em cada conexão. A política deve equilibrar segurança e usabilidade.

Ações críticas podem exigir step-up authentication ou nova aprovação.

18. STEP-UP AUTHENTICATION

Step-up solicita fator adicional quando o usuário executa ação de maior risco.

Exemplos incluem acessar break-glass, alterar política ou abrir cofre crítico.

A aplicação precisa suportar o mecanismo. Não deve interromper tarefas em ponto inseguro.

19. MFA PARA RDP E SSH

RDP e SSH podem ser protegidos no gateway, PAM ou sistema operacional.

Instalar plugins diretamente em servidores OT exige teste de compatibilidade. Preferir controle no caminho intermediário reduz alterações no ativo.

Acesso local de contingência precisa de política separada.

20. MFA PARA APLICAÇÕES LEGADAS

Aplicações antigas podem não suportar SAML, OIDC ou RADIUS.

Um proxy, PAM, VDI ou jump server pode adicionar MFA antes da aplicação.

O controle não deve ser contornável por acesso direto. Firewalls precisam forçar o caminho protegido.

21. MFA E RADIUS

RADIUS pode integrar VPN, Wi-Fi e equipamentos com servidores de MFA.

O RADIUS e 802.1X trata autenticação de rede e certificados.

Fluxos precisam considerar timeout. Uma aprovação demorada pode exceder o tempo do cliente RADIUS.

MFA deve proteger o caminho completo de acesso remoto.

VPN, dispositivo, identidade, PAM, jump server, sessão e destino precisam aplicar políticas coerentes; autenticar forte e liberar a rede inteira continua sendo um risco.

Conhecer o serviço de Projeto de Telecomunicações

22. MFA PARA FORNECEDORES

Cada fornecedor deve possuir identidade individual, fator próprio e período de validade.

Contas compartilhadas ou tokens compartilhados eliminam atribuição.

O acesso deve ser ativado somente durante a tarefa e limitado por PAM ou ZTNA.

Mudanças de equipe do fornecedor precisam revogar identidades imediatamente.

23. ENROLAMENTO DE FATORES

Enrolamento associa o fator ao usuário. O processo precisa confirmar identidade.

Permitir enrolamento apenas com senha comprometida pode dar ao atacante um novo fator.

A primeira ativação pode exigir presença, chamada validada, gestor ou credencial prévia forte.

Eventos de enrolamento devem ser registrados e alertados.

24. RECUPERAÇÃO DE CONTA

Recuperação é frequentemente o ponto mais fraco. Um processo simples de help desk pode contornar MFA.

A política deve exigir verificação suficiente, registrar atendente e usuário e notificar o titular.

Códigos de recuperação precisam ser protegidos. Fatores temporários devem expirar.

25. PERDA OU TROCA DE DISPOSITIVO

O usuário precisa comunicar perda. O fator é revogado e um novo é emitido.

A troca não deve manter o fator antigo indefinidamente. A organização precisa inventariar dispositivos ativos.

Para equipes de plantão, tokens de reserva podem ser mantidos sob custódia.

26. BREAK-GLASS

Contas break-glass permitem acesso quando MFA ou identidade central está indisponível.

Devem possuir escopo mínimo, senha forte, proteção física ou cofre e alerta de uso.

O procedimento precisa ser testado. O PAM pode custodiar as credenciais.

27. DISPONIBILIDADE DO SERVIÇO MFA

Servidores, conectores, push, SMS, PKI e internet podem ser dependências.

A perda do serviço não pode resultar em liberação irrestrita. Políticas de contingência devem ser definidas por aplicação.

A arquitetura pode usar redundância, tokens offline e certificados.

28. AUTENTICAÇÃO OFFLINE

Estações isoladas ou sem internet podem utilizar smart card, certificado, TOTP local ou cache controlado.

O modo offline precisa de limite e revogação. Um fator revogado pode continuar válido enquanto o dispositivo não sincroniza.

Subestações remotas exigem análise de cobertura e enlaces.

29. CONDITIONAL ACCESS

Políticas condicionais consideram usuário, dispositivo, localização, risco e aplicação.

Um acesso privilegiado pode exigir dispositivo gerenciado, MFA forte e origem conhecida.

Condições precisam ser transparentes e testadas. Bloqueios inesperados durante contingência devem ter procedimento.

30. DEVICE TRUST

Confiar no dispositivo envolve certificado, postura, EDR, criptografia e gestão.

MFA de usuário em notebook comprometido não elimina o risco. O EDR e XDR em OT complementa a proteção.

Acesso de fornecedores pode utilizar VDI ou estação controlada em vez do notebook externo.

31. CONTAS DE SERVIÇO

Contas de serviço não utilizam MFA interativo. Devem usar certificados, identidades gerenciadas, cofres ou segredos rotacionados.

Não se deve excluir uma conta de políticas sem controles alternativos.

Uso interativo de conta de serviço deve gerar alerta.

32. CONTAS LOCAIS

Equipamentos e servidores podem manter contas locais para contingência.

Essas contas precisam de senha única, cofre, rotação e logs. Não devem ser utilizadas no cotidiano.

MFA pode ser aplicado no jump server mesmo quando o destino não suporta.

33. SEGURANÇA DO SERVIDOR MFA

O serviço de MFA e identidade é crítico. Precisa de hardening, atualização, backup e administração protegida.

Administradores do MFA devem utilizar método resistente a phishing e PAM.

Alterações de política, fator e integração devem gerar logs.

34. LOGS E MONITORAMENTO

Eventos incluem sucesso, falha, negação, timeout, enrolamento, revogação e recuperação.

O SIEM deve correlacionar origem, aplicação, usuário e dispositivo.

Aprovação após várias negações, acesso de país incomum e novo fator seguido de login são sinais de risco.

35. POLÍTICAS POR CRITICIDADE

Nem toda aplicação exige o mesmo método. A criticidade define fatores aceitáveis.

Acesso ao SCADA, PAM e administração de identidade deve evitar SMS quando alternativas fortes existem.

Aplicações de menor risco podem utilizar TOTP. A matriz de autenticação registra o padrão.

36. EXPERIÊNCIA DO USUÁRIO

MFA excessivamente frequente induz atalhos e fadiga. Sessões, reautenticação e step-up devem ser equilibrados.

“Lembrar dispositivo” precisa de prazo e requisitos de postura. Dispositivos compartilhados não devem receber confiança duradoura.

Treinamento orienta usuários a rejeitar solicitações inesperadas.

37. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir aplicações, usuários, fatores, PKI, integrações, contingência, recuperação e logs.

A matriz relaciona criticidade, método primário, fallback e tempo de sessão.

Dependências de internet, SMS, NTP, diretório e dispositivos precisam ser identificadas.

38. IMPLANTAÇÃO POR ETAPAS

A implantação começa por administradores, VPN, PAM e acesso remoto.

Usuários são enrolados antes da exigência. Pilotos testam aplicações e suporte.

Métodos fracos podem ser mantidos temporariamente com data de retirada.

39. COMISSIONAMENTO E ACEITE

Os testes devem cobrir autenticação, phishing resistance quando aplicável, recuperação e indisponibilidade.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve comprovar segurança e continuidade.

Recuperação e indisponibilidade fazem parte do aceite.

Perda de token, expiração, revogação, falha do serviço, break-glass, logs e fatores alternativos precisam ser testados antes de depender do MFA em operação.

Conhecer o serviço de Comissionamento e Aceite Técnico

40. DIAGNÓSTICO DE FALHAS

TOTP rejeitado pode indicar horário, semente ou janela. Push ausente pode envolver internet, notificação ou registro do dispositivo.

RADIUS timeout pode ser menor que o tempo de aprovação. Certificado rejeitado pode envolver cadeia, validade, EKU ou confiança.

Bloqueio por política condicional exige analisar usuário, dispositivo, localização e risco.

41. ERROS COMUNS

Erros frequentes incluem tratar SMS como proteção máxima, permitir enrolamento fraco e não testar recuperação.

Também são comuns contas compartilhadas, MFA somente na VPN com acesso amplo e break-glass nunca testado.

Outro erro é exigir push repetidamente, aumentando fadiga e aprovações automáticas.

42. CONCLUSÃO

MFA reduz o risco de credenciais roubadas ao exigir fatores independentes. A segurança varia conforme o método, enrolamento, recuperação e resistência a phishing.

Em OT, MFA deve proteger VPN, PAM e acesso privilegiado sem criar indisponibilidade. Métodos fortes, contingência controlada, logs e segmentação permitem confirmar identidade sem transformar o fator em única barreira de segurança.

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-63B — Digital Identity Guidelines: Authentication and Lifecycle Management.

[2] W3C. Web Authentication: An API for accessing Public Key Credentials.

[3] FIDO ALLIANCE. FIDO2 specifications and deployment guidance.

[4] M'RAIHI, D. et al. RFC 6238 — TOTP: Time-Based One-Time Password Algorithm. IETF, 2011.

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

[6] CISA. Implementing Phishing-Resistant MFA guidance.

O que é MFA? MFA é autenticação com dois ou mais fatores de categorias diferentes.**Qual é a diferença entre MFA e 2FA?** 2FA utiliza exatamente dois fatores. MFA pode utilizar dois ou mais.**TOTP é seguro?** TOTP melhora a proteção, mas pode ser capturado em phishing em tempo real. FIDO2 oferece maior resistência.**SMS é um bom segundo fator?** É melhor que senha isolada, mas possui limitações e não é preferível para acessos privilegiados quando existem métodos fortes.**O que é MFA fatigue?** É o abuso de notificações push para induzir o usuário a aprovar uma solicitação indevida.**O que é FIDO2?** É um padrão de autenticação por criptografia assimétrica resistente a phishing.**MFA deve ser usado na VPN?** Sim, especialmente para acesso remoto. A autorização após a VPN também deve ser limitada.**Como aplicar MFA a uma aplicação legada?** Pode-se usar PAM, jump server, proxy ou gateway que exija MFA antes da aplicação.**O que é break-glass?** É uma conta emergencial protegida e monitorada para uso quando o serviço normal está indisponível.**Como testar MFA?** Devem ser testados

fatores válidos e inválidos, recuperação, perda de dispositivo, falha do serviço, break-glass e logs.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas