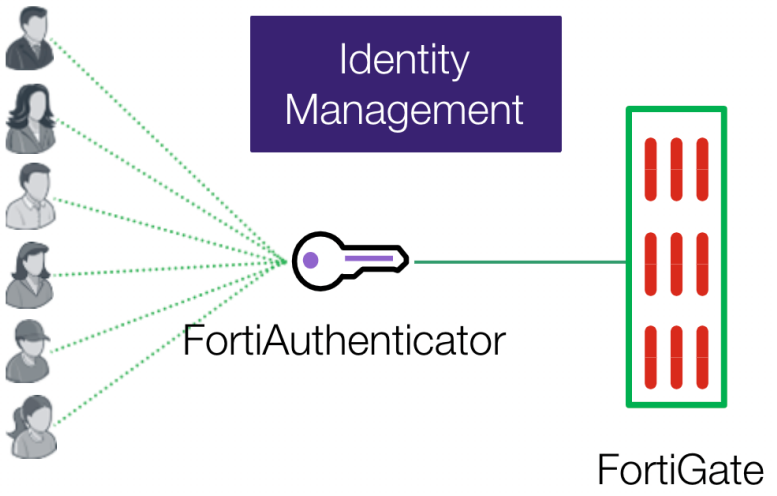
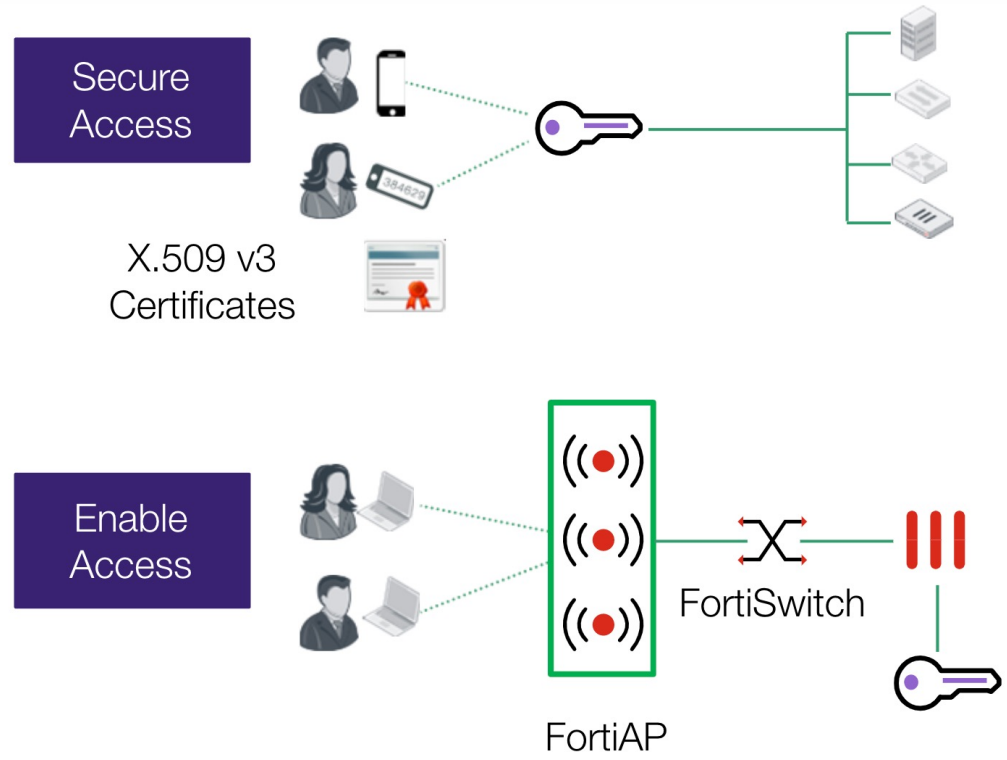

hackone
FORTIAUTHENTICATOR
NOME DO MENTOR: ALEXANDRE SABINO

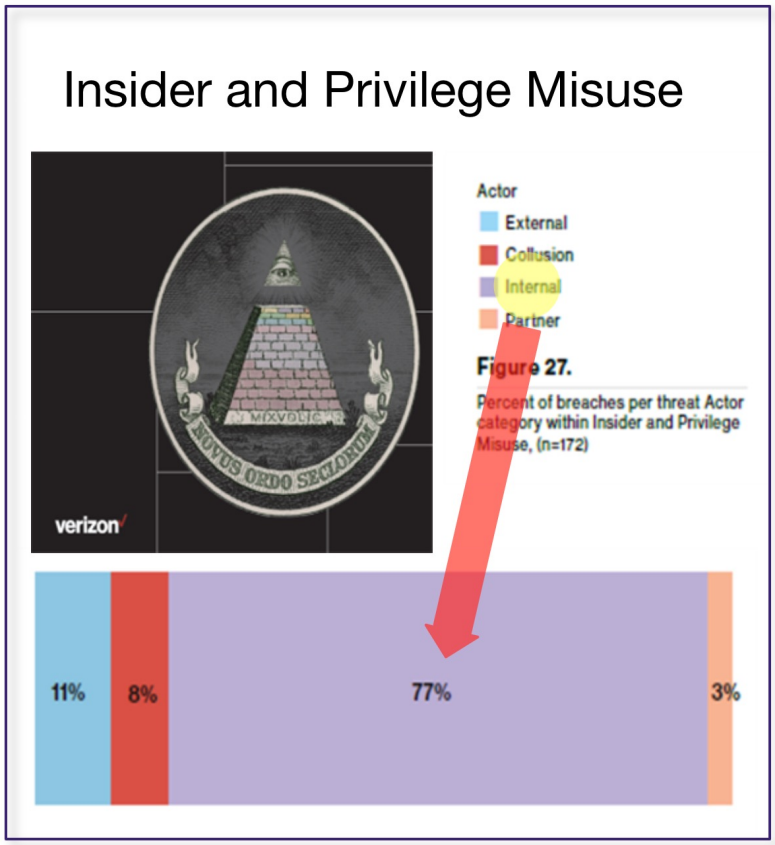
O QUE É FORTIAUTHENTICATOR?

FortiAutheticator é um produto enterprise de gerenciamento de identidade, que fornece fortes autenticações e autorizações para uma rede conectada



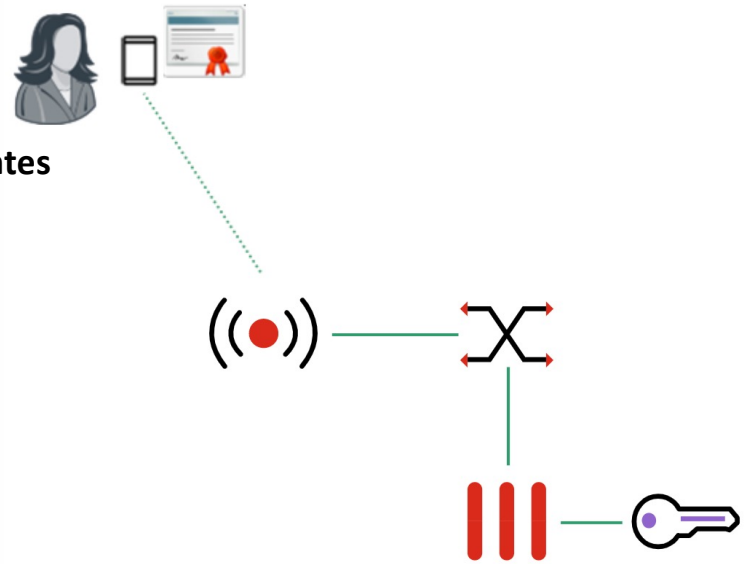


PROBLEMAS E AS DORES DOS CLIENTES



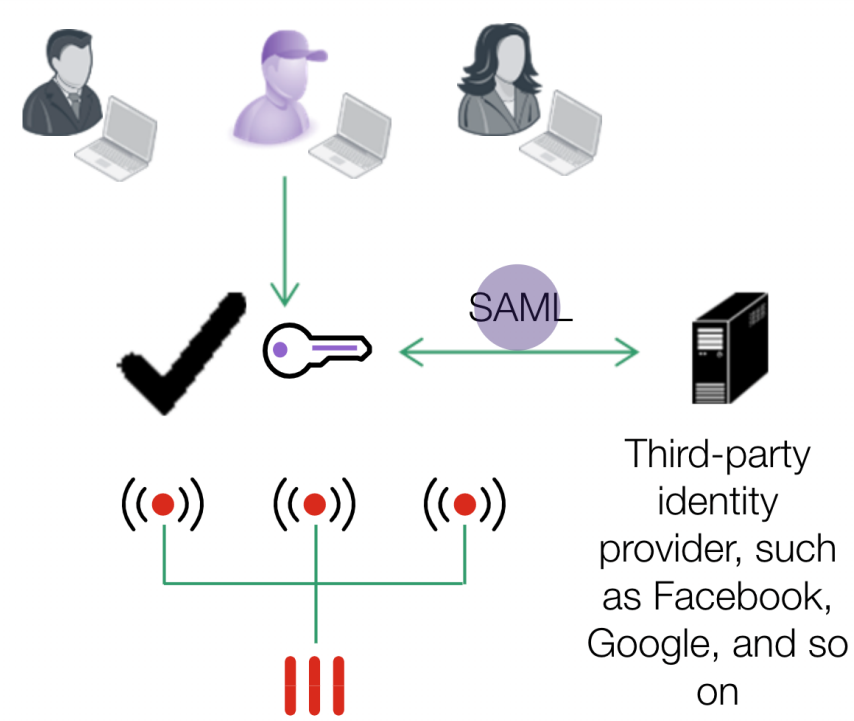
HABILITAR AUTENTICAÇÃO DE ACESSO PARA REDE WIFI E CABEADA

- **Autenticar usuários e máquinas**
- **Autenticação de dispositivos baseada em certificados em ambientes BYOD**
- **Método de autenticação de visitantes:**
  - Autenticação por certificado
  - Password challenges
  - Funções de Captive Portals
- **Autenticação 802.1X**



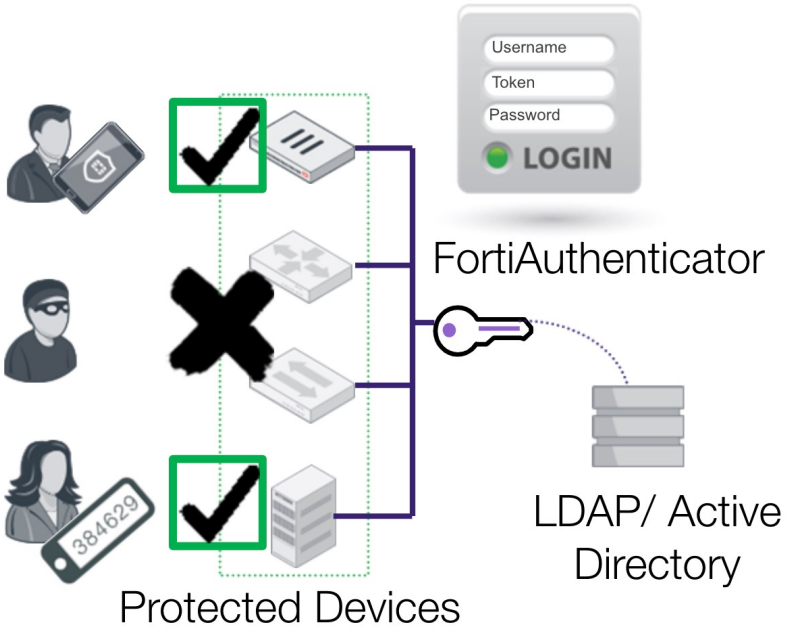
HABILITAR ACESSO PARA GERENCIAMENTO DE VISITANTES

- **Gerenciamento de visitantes:**
  - Self-Registration
  - Autenticação através de mídias sociais:
    - Facebook, Google, Twitter e LinkedIn
  - Outras opções incluem:
    - Envio de SMS para comprovar a identidade
    - Opção de cadastro pela recepção
  - Limitação de tempo
  - Apagar contas expiradas



ACESSO SEGURA ATRAVÉS DE MULTI-FACTOR AUTHENTICATION (MFA)

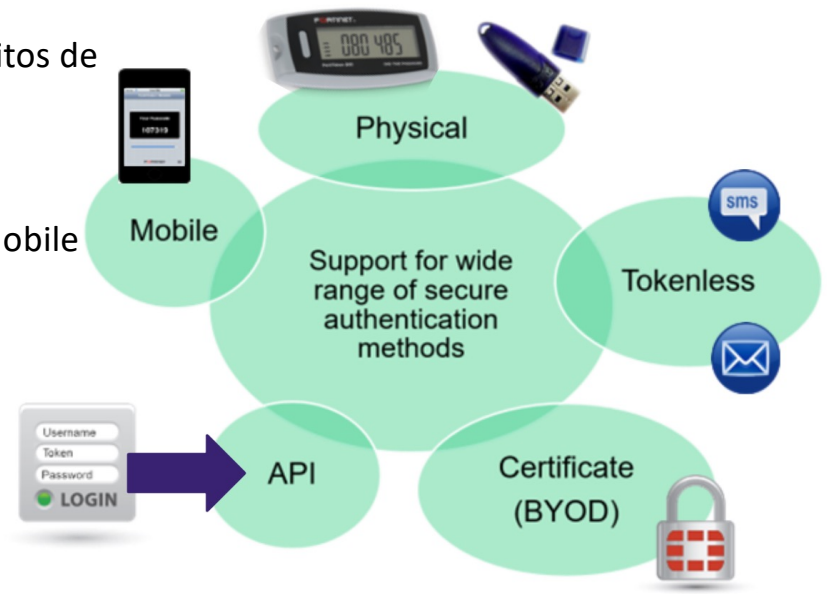
- **Multi-fator authentication (MFA):**
  - Autenticação fortalecida usando:
    - Algo que o usuário conhece, tem e é
  - Reduz a sobrecarga operacional
    - Integração com LDAP e Active Directory
  - Self-Service password reset
  - Workflow integrado de token perdido



ACESSO SEGURO ATRAVÉS DE (MFA)

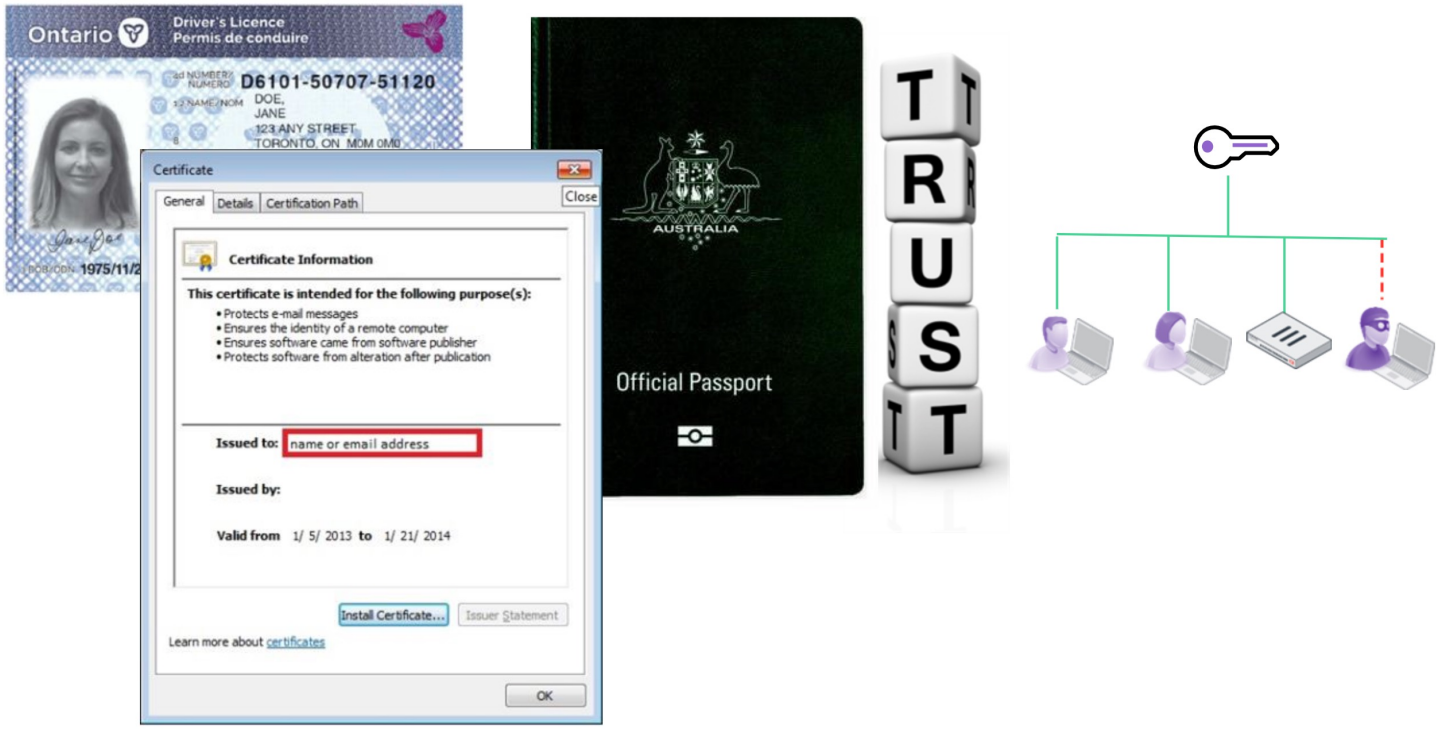
TOKEN AND ONE-TIME PASSWORD AUTHENTICATION

- **Two-Factor Authentication (2FA)**
  - Diferentes tipos de Tokens para atender todos os requisitos de implementação
    - OATH-Based, TOTP (time) – based tokens (FTK200)
    - USB Certificate Tokens (FTK300)
    - FortiToken Mobile para Android, iOS e Windows Mobile
    - SMS e email Tokens
    - Cisco, F5, Citrix, entre outros
    - Suporta qualquer dispositivo que suporte Radius
    - Microsoft Windows Domain e OWA



ACESSO SEGURO ATRAVÉS DE (MFA)

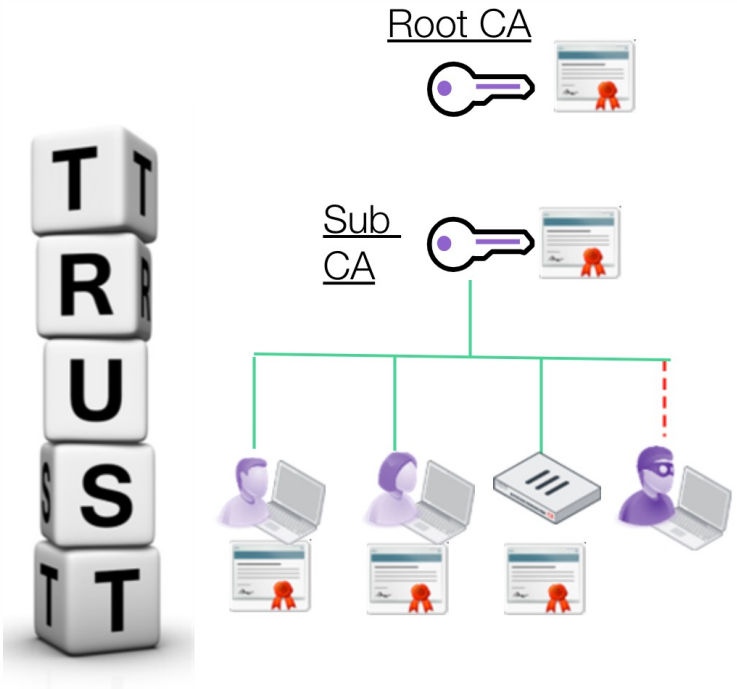
CHAIN OF TRUST IN CERTIFICATE AUTHENTICATION



ACESSO SEGURO ATRAVÉS DE (MFA)

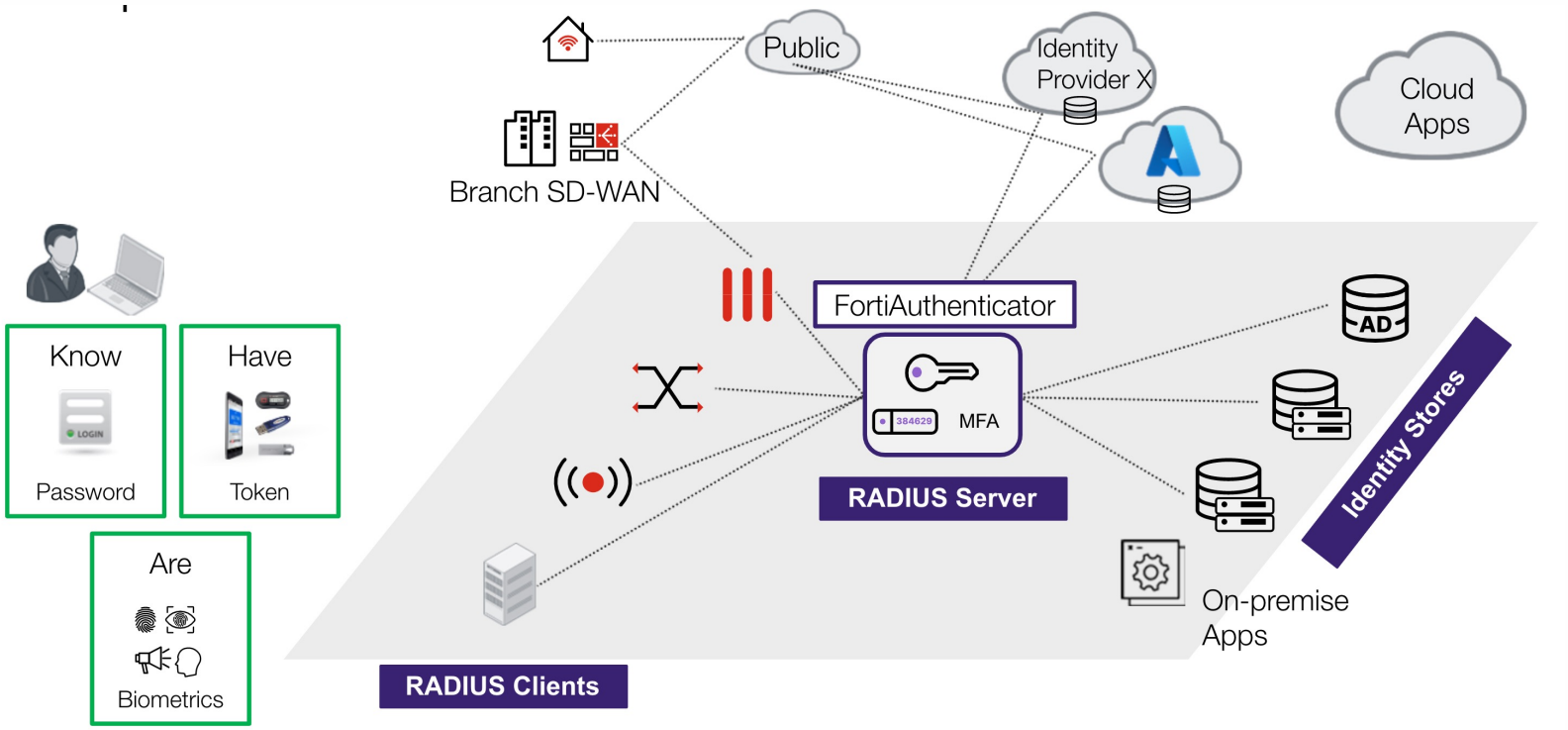
CHAIN OF TRUST IN CERTIFICATE AUTHENTICATION

- **Certificate (ou Certification) Authority:**



ACESSO SEGURO ATRAVÉS DE (MFA)

ADAPTATIVE AUTHENTICATION

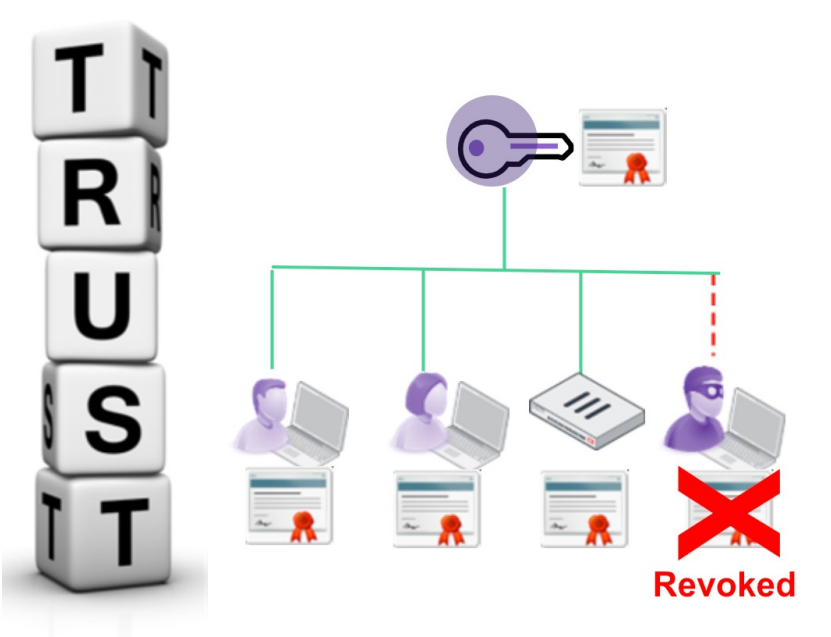


ACESSO SEGURO ATRAVÉS DE (MFA)

A MÁQUINA DE AUTENTICAÇÃO DE CERTIFICADOS

- **Certificate (or Certification) authority (CA):**
  - Emissão de certificados para múltiplos usuários
    - Rede sem fio e cabeada usando 802.1x (PEAP, EAP)
    - Autenticação de Desktop Windows

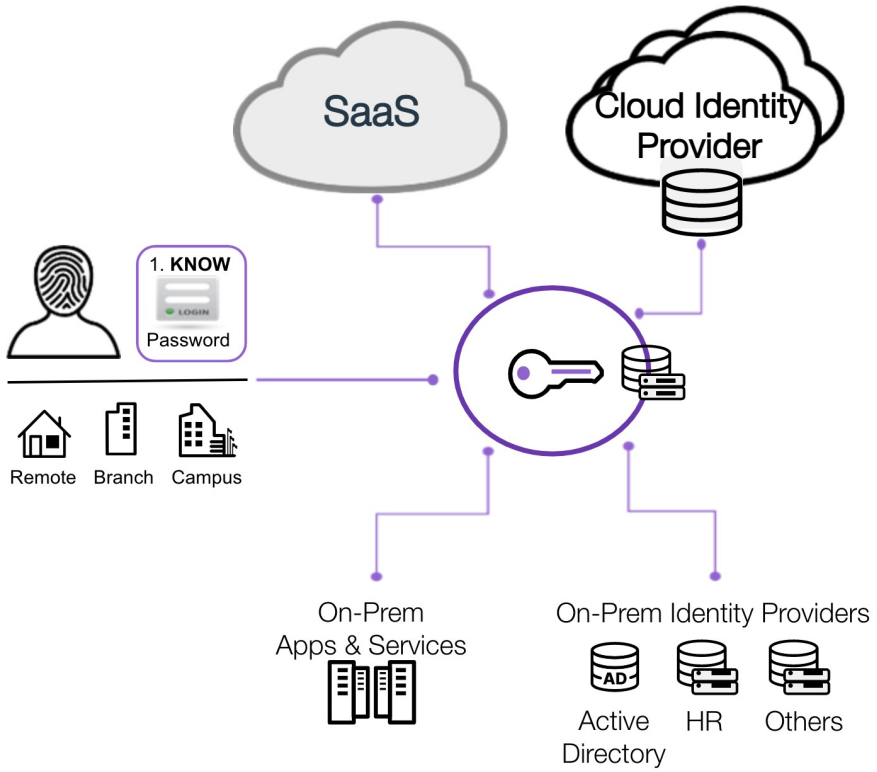
- **Autenticação VPN**
  - Certificado para VPN
    - Revogar certificados se dispositivo foi perdido (OSCP)
    - Distribuição de certificados com Zero Touch (SCEP)
    - Public Key Infrastructure (PKI)
    - Integração com o FortiManager para simplificar a implementação



AUTENTICAÇÃO CENTRALIZADA

HABILITA ACESSO SEGURO PARA TODOS OS USUÁRIOS

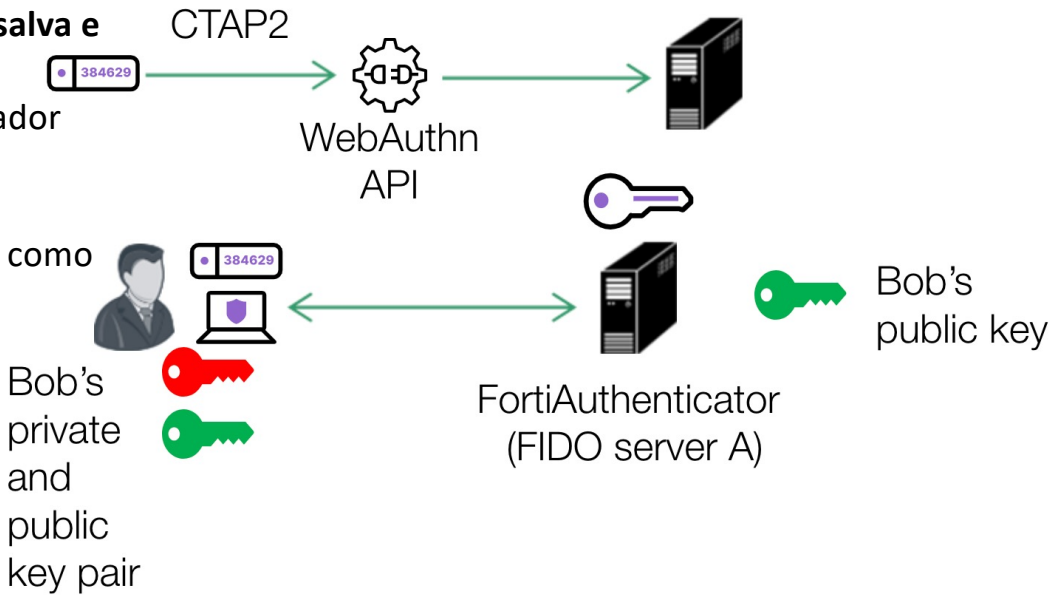
- **Um usuário ou dispositivo aproveita as credenciais existentes em um site para autenticar em outro**
- **Componentes de uma autenticação centralizada:**
  - Entidade final (usuário ou dispositivo)
  - Service Provider (SP) ou Identity Provider Proxy
  - Identity Provider (IdP)
- **FortiAuthenticatior poder ser um SP ou IdP**
- **Aproveita as nuvens IdP, tais como Google, Facebook e outros sites públicos que gerenciam *Personally Identifiable Information* (PII)**
- **Utiliza Security Assertion Markeup Language (SAML) e outros formatos de dados**



ACESSO SEGURO ATRAVÉS MFA

PASSWORDLESS FIDO2 AUTHENTICATION

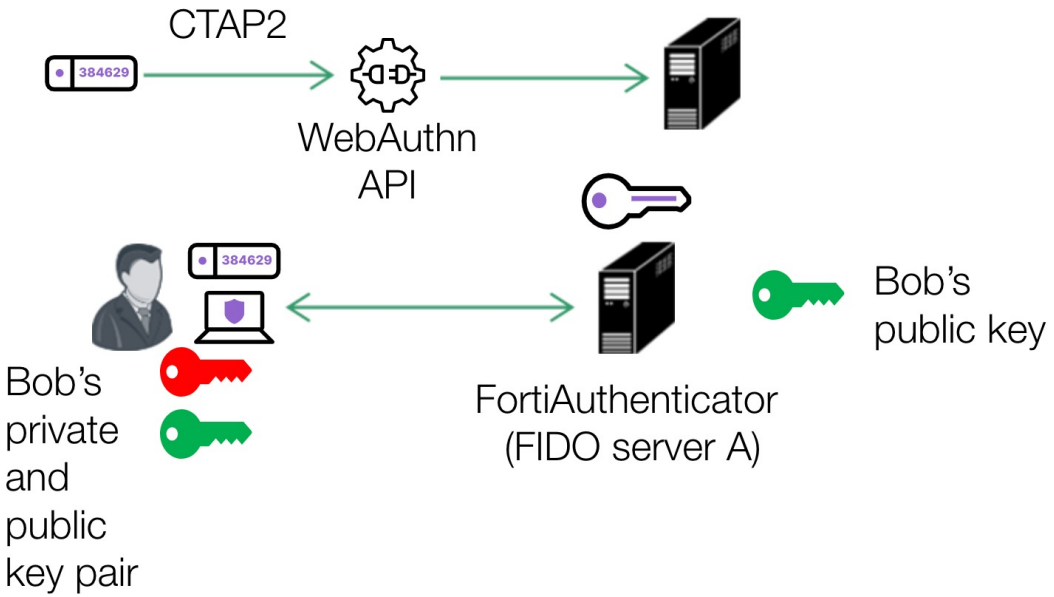
- **Secure Key Store é chamado de autenticador que salva e guarda os acesso para as chaves de criptografia**
  - Um autenticador interno está em um computador
    - Exemplo: Windows Hello
  - Um autenticador externo (também conhecido como um roaming) é um dispositivo que conecta ao computador
  - Exemplo: FortiToken 400



ACESSO SEGURO ATRAVÉS MFA

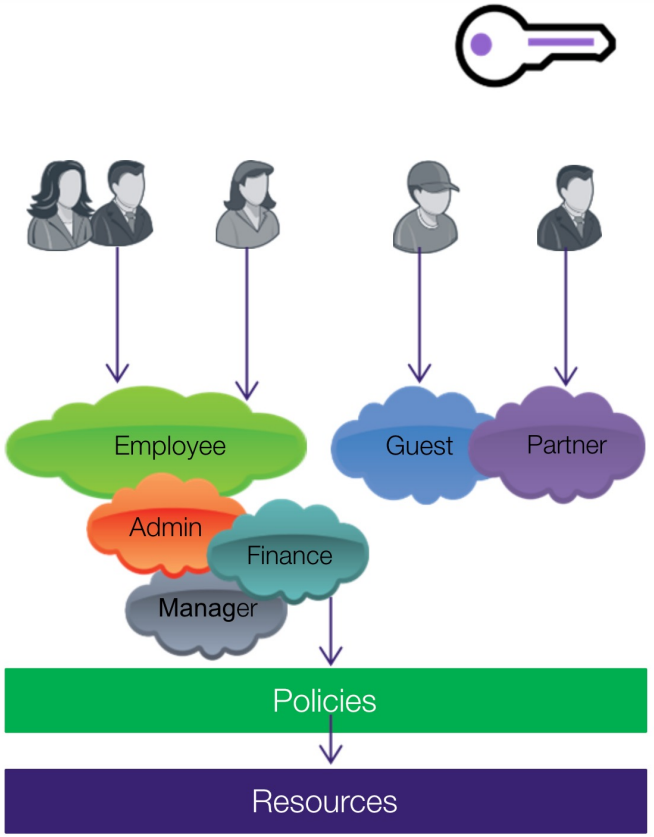
PASSWORDLESS FIDO2 AUTHENTICATION

- **Servidor FIDO envia um desafio ao cliente**
- **Cliente assina o desafio com a chave privada do usuário e retorna o desafio**
- **Servidor verifica a assinatura no desafio usando a chave pública do usuário**



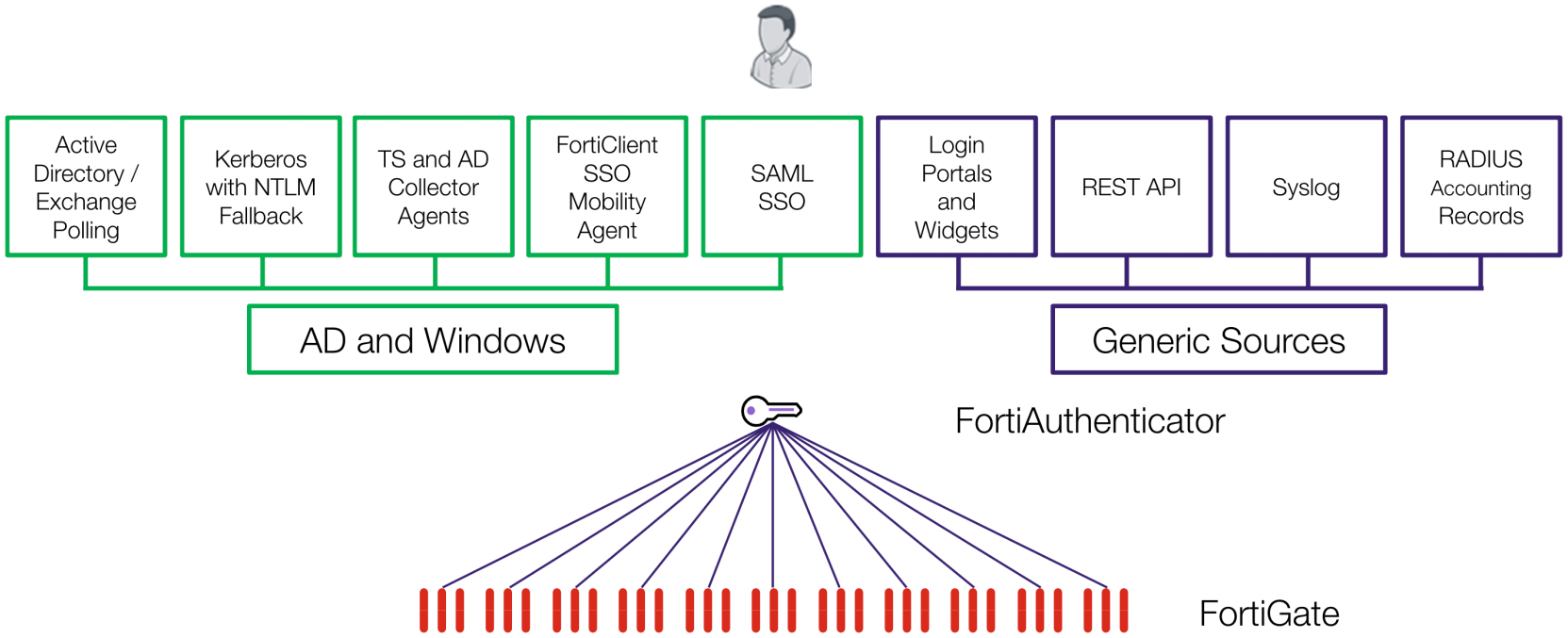
GERENCIANDO IDENTIDADES COM FSSO

- **Fortinet Sigle Sign-on**
  - Identifica os usuários e aplica políticas de segurança baseadas no usuário
    - Coleta informações da identidade do usuário
    - Controle granular da rede e dos acessos às aplicações
    - Permite que o FortiGate, FortiClient, FortiMail e FortiCache apliquem políticas apropriadas baseadas na identidade e regras do usuário



GERENCIANDO IDENTIDADES

FORTINET SSO



GERENCIANDO IDENTIDADES

HA E ESCALABILIDADE

- **High Availability (HA) e Escalabilidade**
  - Active-Passive HA
    - Suporta todas as funcionalidades
  - Active-Active config sync
    - Distribuição Geográfica
    - Balanceamento de carga através dos dispositivos
    - Suporta uma funcionalidade de sincronismo de autenticação
    - Pode ser combinado com Active-Passive HA


hackone