O PROAPPS 2-FA (TWO-FACTOR AUTHENTICATION SYSTEM)

O ProApps 2-FA (Two-factor Authentication System) é uma solução robusta de implementação de autenticação forte fundada no mínimo em 2 fatores de autenticação. A solução é composta dos seguintes componentes:

- **SAE:** é o motor de autenticação forte (strong authentication engine), que implementa toda a lógica do processo de autenticação baseada em múltiplos fatores. É composta de um sistema de gestão de identidade mínimo para sustentar a base de informação inerente a autenticação do usuário; é o gerador lógico das senhas e hashs OTP;

- **GUI:** interface gráfica com o usuário que permite administração geral da solução;

- **Action Provider:** webservice de automação de operações de CRUD (Criação, Leitura, Atualização e Remoção, do acrônimo em inglês) padrão RESTful JSON; adequado para realizar todas as operações de preparação e solicitação de segundo fator de autenticação; é a interface que permite o disparo remoto do processo de autenticação forte; permite interoperabilidade da solução com produtos legados e de terceiros;

- **2-FA Delivery:** é a interface que realiza a entrega de fato do segundo fator de autenticação; tipicamente é composto de um agente de envio de mensagens SMS por celular, smartphones iPhone, Android ou tablets iPad e Android; pode em casos especiais ser senhas sequenciais não reutilizáveis impressas em papel ou cartão;

O ProApps 2-FA (Two-factor Authentication System) implementa padrões de fato da indústria, com destaque a: RFC-4226; RFC-6238; RFC-2104; OPIE; FIPS-180/4; padrão formal 2-FA OTP Time Based e Event Based;

Padrões Formais de Mercado & Conformidade com Requisitos Fortes

Compatível com OTP 2-FA Google, Apple, Dropbox, Twitter, Facebook; provisionamento web; provisionamento por QR-Code compatível com Google e Próprio; Hash Pass baseado em sha256 e sha512, atende requisitos extremos da NSA, incluindo FIPS-180; compatível BAE Systems STOP/XTS400; atende requisitos militares; atende requisitos da marinha mercante e de guerra;

Autenticação Forte (terceiro e quarto fatores de autenticação)

- **3-FA:** terceiro fator de autenticação pode ser implementado através de geolocalização apoiada por GPS interno do aparelho ou triangulação; o raio de cobertura é configurável no SAE a partir de um ponto de georeferência; depende do smartphone ter portanto recurso de geo-localização; 3-FA com

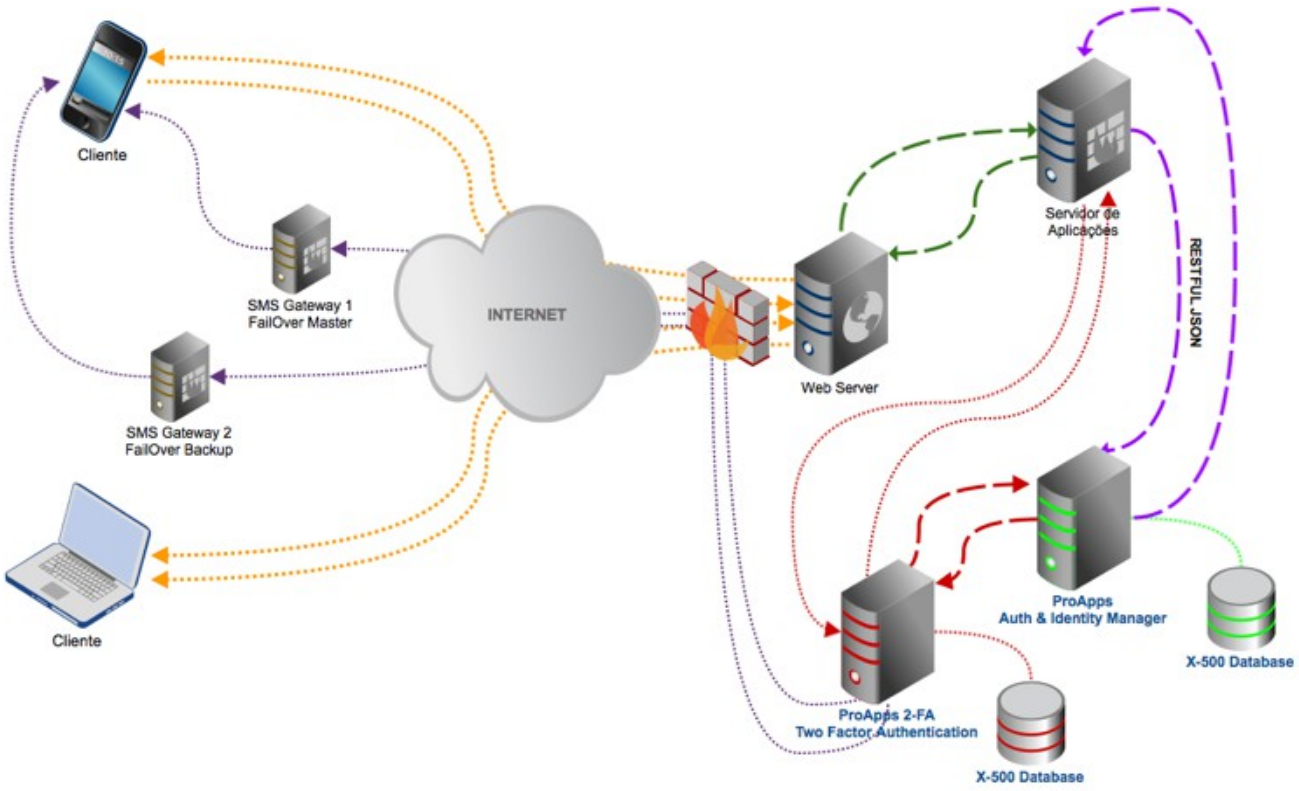
provisionamento plenamente suportado quando usado com sistema de integração e unificação de autenticação ProApps; as ações principais do terceiro fator de autenticação é submeter a coordenada GPS para o webservice afim de auditoria e tomada de decisão na lógica de negócio, e/ou (parametrizável) simplesmente se recusar a desbloquear a criptografia AES-256 (de hardware) não liberando acesso a contra-chave OTP se a geolocalização estiver indisponível, fora do raio autorizado, ou a informação geográfica não vier de uma fonte esperada;

- **4-FA:** o acesso ao token quando o método de Delivery for smartphone pode ainda testar reconhecimento facial e biometria quando disponível e principalmente desejado, reforçando os demais fatores de autenticação forte;

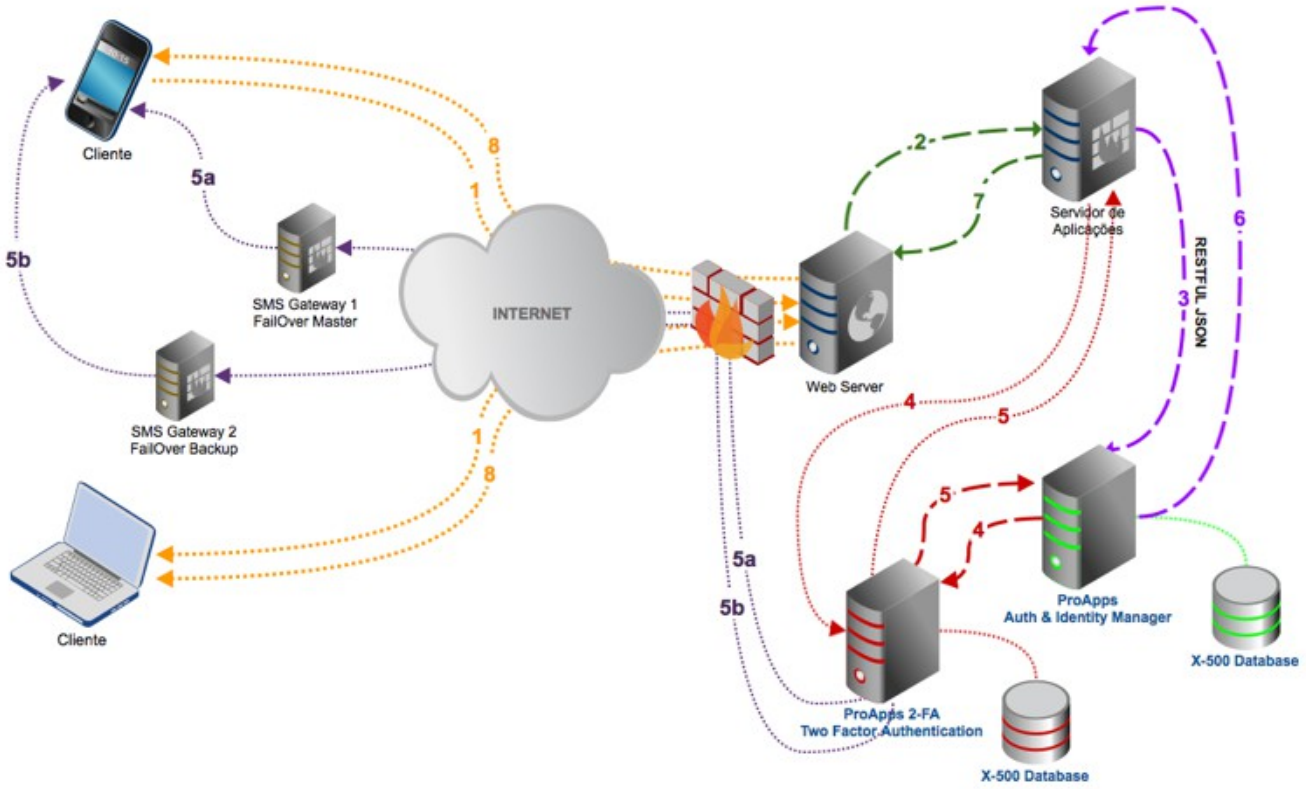
Além disso, a solução prevê alta disponibilidade, suportando VRRP e licenciamento sempre duplo para redundância e HA. E se você já tem algum módulo ProApps implantado, como ProApps Auth & Identity Manager;

Diagrama Funcional Lógico

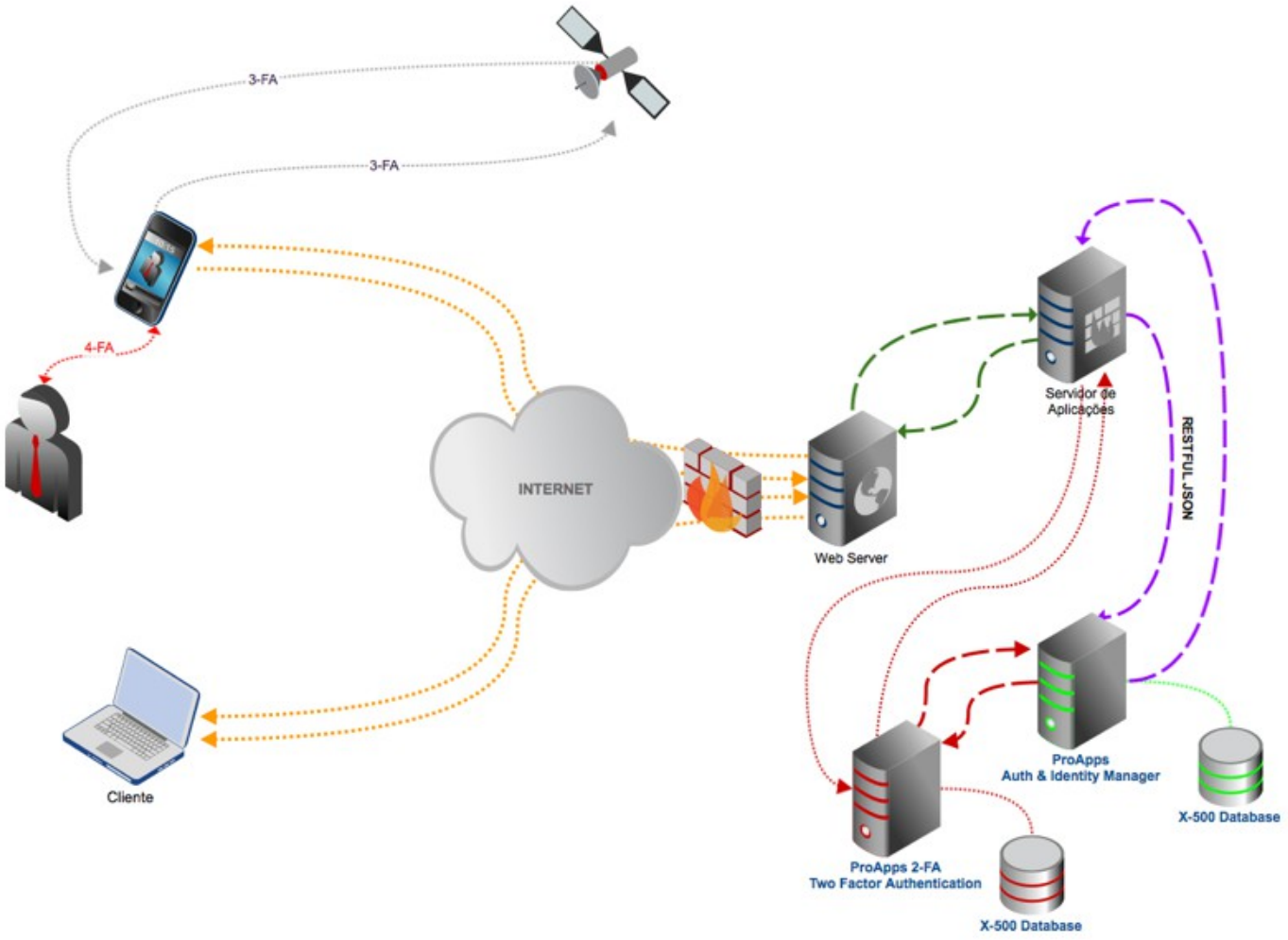
Diagrama incluindo integração com ProApps 2-FA



Fluxo lógico ilustrativo para a solução



Terceiro e quarto fatores de autenticação (3-FA & 4-FA)



Token Smartphone Incluso (Out of Band)

A solução de 2-FA Delivery baseada em token de *smartphone* ou *tablet* soma toda a praticidade de uma solução *offline,* pois não depende de rede de dados nem telefonia para receber SMS, após provisionamento, com a melhor relação de custo/benefício pois difunde a prática de BYOD (dispositivo do próprio cliente), diminui custos com mensagens SMS, enquanto mantém fator equivalente de segurança, permitindo estratégias seguras de provisionamento de segredo no *token* tanto por autenticação de hardware, por SMS, ou ainda por provisionamento seguro via *web* e até mesmo por provisionamento QR-Code seguro.

Os dados de segredo são armazenados no dispositivo, protegido com criptografia AES-256, criptografia essa, acelerada por hardware.

E o mais importante, a oferta de Token OTP para smartphones Apple e dispositivos baseados em Android é parte integral e completa de nossa oferta de solução. Não oferecemos apenas componentes ou métodos de acesso e uso da estratégia de segurança 2-FA.

Nós entregamos o produto, pronto, funcional, com identidade visual customizada para nossos clientes, e refletindo o fluxo de provisionamento escolhido e definido pelo cliente conforme suas prioridades e seu processo de negócio. Da sua infra-estrutura de 2-FA ao *token* final publicado na App Store e Google Play, nós cuidamos de todos os aspectos da sua solução de segundo (e múltiplos) fatores de autenticação!