

BioPassID

Manual de implantação

O BioPass ID é um serviço online baseado em nuvem que fornece uma poderosa tecnologia multibiométrica (reconhecimento de impressões digitais e face) para os desenvolvedores de qualquer serviço, software ou plataforma com acesso a Internet. Como se trata de um serviço de computação em nuvem, é possível dimensionar dinamicamente todos os requisitos de desempenho e de armazenamento, tornando a solução aplicável a uma ampla gama de cenários de uso.

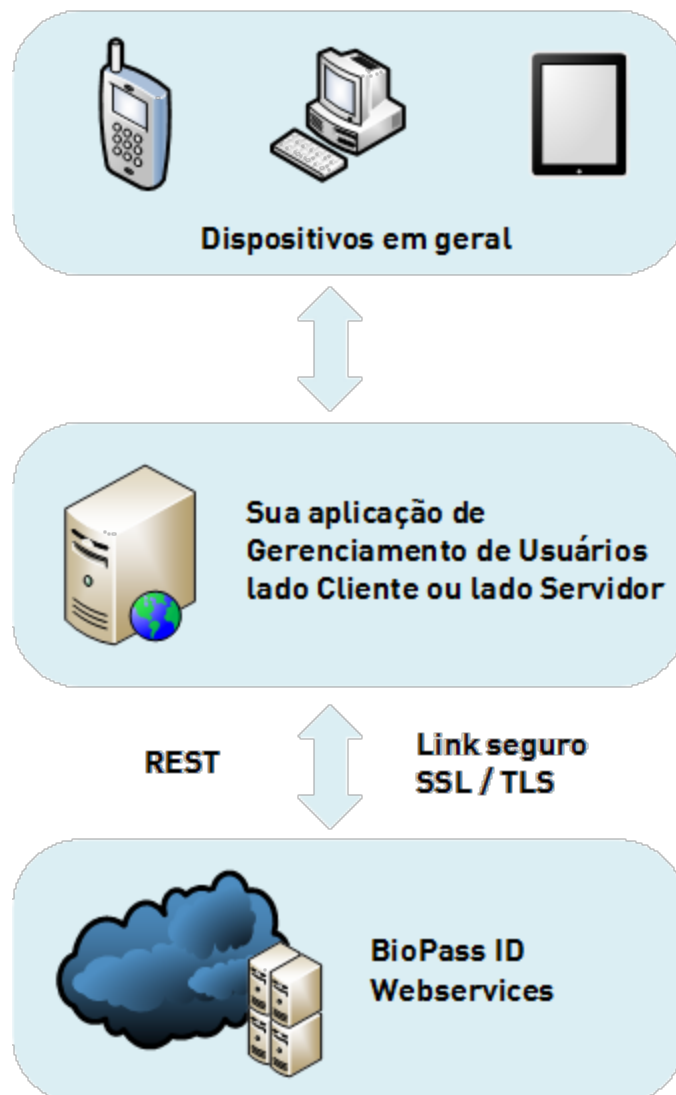


Diagrama de de arquitetura da plataforma

Integração com seu software

O BioPass ID tem como objetivo prover a sua aplicação a capacidade de validar a identidade de uma pessoa através de seus dados biométricos. Para isso, se faz necessária a integração com seu(s) software(s) de cadastro de pessoas e de validação/ autenticação de identidade. As operações ou funcionalidades disponibilizadas pelo BioPass ID para integração com sua aplicação são:

- Adição / alteração de pessoa;
- Exclusão de pessoa;
- Verificação de pessoa (1:1);
- Identificação de pessoa (1:N).

As funcionalidades do BioPass ID são acessíveis através de uma API (*Application Programming Interface*) do tipo REST (*Representational State Transfer*). Portanto, elas devem ser implementadas através de integração com o seu software, independente de plataforma ou linguagem de programação. Consulte a documentação da API do BioPass ID para mais detalhes.

É importante lembrar que o BioPass ID é um serviço baseado em nuvem e portanto as chamadas a sua API dependerem de conexão com a Internet. O desenvolvedor deve analisar em qual ponto de sua aplicação irá implementar as funções da API podendo ser diretamente em um dispositivo cliente ou em um servidor de aplicação responsável por processar as requisições do cliente e submetê-las ao BioPass ID.

CustomID

Durante a adição de uma pessoa ao BioPass ID você pode atrelar a ela um código personalizado que será utilizado para identificá-la em sua aplicação o qual chamamos de *CustomID*. Este campo é alfanumérico e é limitado a até 50 caracteres. Você pode utilizar um código interno de seu sistema, um CPF, um número de cartão, etc. O importante é que seja um número de identificação único da pessoa em sua base de dados.

BioPassID

Também durante a adição de uma pessoa é retornado o código interno dela na plataforma BioPass ID, o qual chamamos de *BioPassID*. Você também pode opcionalmente utilizar esse código para identificar a pessoa de forma única em seu sistema.

Integração no cadastro de pessoas



Diagrama de cenário de cadastro exemplo

Sua aplicação de cadastro de pessoas será responsável por coletar os dados biométricos dos indivíduos e submetê-los a plataforma BioPass ID para processamento.

Basicamente sua aplicação deverá:

- Coletar as impressões digitais através de sensor biométrico de digitais;
 - O BioPass ID suporta até as 10 impressões digitais de um indivíduo, cabe ao desenvolvedor decidir quais coletar para cadastro. Indicamos o cadastramento de todas para flexibilidade na hora da validação permitindo que o usuário possa utilizar qualquer uma das suas impressões digitais. A utilização de todas também garante que determinado ID não contenha impressões digitais de outra pessoa.
- Coletar a face através de uma webcam ou câmera capaz de gerar imagens de no mínimo 640 x 480 pixels não interpolados;
- Submeter os dados biométricos para identificação (1:N) com o objetivo de verificar a existência de cadastro já existente do indivíduo;
- Caso não exista cadastro anterior, submeter os dados biométricos para adição na plataforma BioPass ID juntamente com o CustomID do indivíduo para futura identificação em seu sistema;
- Processar o retorno de cada transação submetida ao BioPass ID após processamento.

Integração na validação de identidade de pessoas



Diagrama de cenário de validação exemplo

Sua aplicação pode necessitar validar a identidade de uma pessoa em vários pontos. Em todos esses pontos será necessário coletar os dados biométricos do indivíduo e submetê-los a plataforma BioPass ID para processamento.

Sua aplicação deverá:

- Coletar uma ou várias impressões digitais através de sensor biométrico de digitais;
 - Quanto mais impressões digitais forem coletadas para validação, melhor será o resultado, porém, se obtém excelentes resultados de verificação de identidade com apenas uma impressão digital com boa qualidade de coleta;
- Coletar a face através de uma webcam ou câmera capaz de gerar imagens de no mínimo 640 x 480 pixels não interpolados;
- Submeter os dados biométricos para verificação (1:1) juntamente com o *CustomID* para validar a identidade do indivíduo;
- Processar o retorno da transação de verificação submetida ao BioPass ID após processamento.

Importante: como o BioPass ID trabalha com o conceito de multibiometria, cabe ao desenvolvedor decidir se irá submeter para validação de identidade apenas as impressões digitais, apenas a face ou o conjunto de dados biométricos. Quanto mais informações forem submetidas, melhor será a qualidade da verificação.

Requisitos de ambiente operacional

O uso do BioPass ID é baseado na chamada a funções de API que é implementada em um conceito de transferência via Internet e possui como requisitos de ambiente o seguinte:

- As camadas da sua aplicação que realizam as chamadas a API do BioPass ID devem ter conexão com a Internet;
- A API pode ser implementada em qualquer sistema operacional, qualquer plataforma de hardware

- através de qualquer linguagem de programação;
- As chamadas remotas a API são realizadas através do protocolo HTTP (*Hypertext Transfer Protocol*) pela porta 80 (porta padrão da Web);
 - Por padrão, o tamanho médio de cada pacote enviado para cadastro do indivíduo, considerando o envio das 10 impressões digitais e da face é de 1,5 Mb, sendo aproximadamente 100 Kb por impressão digital e 500 Kb por face;
 - Impressões digitais em formato PNG;
 - Face em formato JPG com compactação em nível 80;
 - Por padrão, o tamanho médio de cada pacote enviado para verificação, considerando o envio de 1 impressão digital mais a face é de 600 Kb, sendo aproximadamente 100 Kb para a impressão digital e 500 Kb para a face;
 - Impressões digitais em formato PNG;
 - Face em formato JPG com compactação em nível 80;
 - Opcionalmente podem ser utilizadas outras técnicas para redução do uso de banda, tais como:
 - Envio de impressões digitais para identificação ou verificação já convertidas em modelos (templates) biométricos no formato ISO;
 - Envio de impressões digitais para qualquer tipo de transação convertidas no formato WSQ (*Wavelet Scalar Quantization*).

Restrições para coleta de face para reconhecimento facial

O reconhecimento facial é muito sensível à qualidade da imagem. Então, deve-se ter cuidado máximo na aquisição de imagens. As restrições descritas abaixo, se bem aplicadas, podem trazer os melhores resultados possíveis na execução das transações de verificação e identificação com face.

Pose

Deve ser usada a pose frontal (face completa). A rotação da cabeça deve ser menos do que ± 5 graus da frente em todas as direções – para cima/baixo, girada pra esquerda/direita, inclinada para a esquerda/direita.

Expressão

A expressão deve ser neutra (sem sorrir) com os dois olhos abertos, e a boca fechada. Deve-se tentar ao máximo seguir esta especificação. Um sorriso com a mandíbula fechada é permitido, porém não recomendado.

Exemplos de expressões não recomendadas

- Sorriso onde a parte de dentro da boca é exposta (mandíbula aberta).
- Sobrancelhas levantadas.
- Olhos fechados.
- Olhos não direcionados para a câmera.
- Olhar estrábico.
- Franzir a testa/ sobrancelhas.
- Cabelo cobrindo os olhos.

- Armação do óculos cobrindo parte do olho.

Mudanças faciais

Barba, bigode e outras características mutáveis da face influenciam na qualidade do reconhecimento e se mudanças frequentes na face forem típicas a um indivíduo, o banco de dados de face deve ter, por exemplo, a face com barba e totalmente sem barba (barba feita) com ID idêntico.

Iluminação

A iluminação deve ser igualmente distribuída em cada lado da face e da parte superior para a parte inferior. Não deve haver direção significativa da luz ou sombras visíveis. Deve-se tomar cuidado para evitar “hot spots”. Eles são causados tipicamente quando uma fonte focada de luz de alta intensidade é usada para iluminação.

Óculos

Não deve haver iluminação nos óculos. Isto pode ser alcançado tipicamente pelo aumento do ângulo entre a luz, o sujeito e a câmera para 45 graus ou mais. Se as reflexões de iluminação não puderem ser removidas, então os óculos devem ser retirados. (No entanto, isto não é recomendado, uma vez que o reconhecimento da face tipicamente trabalha melhor quando compara pessoas de óculos com elas mesmas usando os mesmos óculos). Óculos devem possuir lentes claras e transparentes de forma que os olhos e as íris sejam claramente visíveis. Óculos fortemente coloridos não são aceitáveis.