

São Paulo, 18 de novembro de 2008.

Consulta Pública sobre Sistemas de Biometria

A FEBRABAN torna público que, durante o período de 24/11/2008 a 27/02/2009, efetuará um levantamento de informações relativas a requisitos técnicos, estimativas de custos, prazos de implementação, entre outras, com a finalidade de avaliar sistemas biométricos para aplicação em sistemas bancários de autenticação.

Para tanto, a FEBRABAN informa que receberá informações, através do e-mail cnab@febraban.org.br, sobre dispositivos biométricos, soluções e sistemas com as características básicas descritas abaixo:

Os sistemas e dispositivos devem ser baseados nas tecnologias biométricas a seguir:

1. Para autenticação de clientes em terminais bancários de auto-atendimento
 - 1.1 Impressão digital
 - 1.2 Padrão da íris
 - 1.3 Padrão vascular de partes da mão.
2. Para autenticação de clientes em outros sistemas
 - 2.1 Voz

Convidamos os fornecedores interessados a nos enviarem as informações solicitadas tendo como guia o questionário anexo.

Atenciosamente,

Wilson Roberto Levorato
Diretor Geral

Gustavo José Costa Roxo da Fonseca
Diretor Setorial de Tecnologia e Automação Bancária

	Solução - Dispositivo biométrico
1. Permanência	A sua solução biométrica está pronta para tratar alterações ocasionadas pelo envelhecimento, pela mudança das condições de saúde, pelo estado emocional, pela utilização e desgaste de partes do corpo, entre outras?
2. Influência ambiental	Quão resistente é a solução à influência ambiental, representada pela resistência e manutenção do desempenho frente a variações ambientais comuns aos locais onde estão instalados os terminais de auto-atendimento do Banco, como as variações de luminosidade, umidade, temperatura, nível sonoro, maresia, poluição, entre outras?
3. População coberta	Qual é o percentual da população brasileira que não possui a característica biométrica utilizada pela sua solução?
4. População coberta	Qual é o percentual da população brasileira que, por não atender aos requisitos mínimos de extração do exemplar, não consegue ser autenticada com a sua solução?
5. Aceitação pública	Qual o grau de aceitação do usuário perante a sua solução? (baixo, médio, alto). Existem pesquisas e trabalhos realizados que comprovem esta afirmação?
6. Robustez	O dispositivo resiste à utilização intensiva? Qual é o tempo de vida útil do dispositivo? Que prazo de garantia pode ser fornecido?
7. MTBF	Qual é o tempo médio entre falhas (MTBF) do dispositivo?
8. Dimensões	Quais as dimensões do dispositivo e dos demais acessórios necessários para utilização no terminal de auto-atendimento?
9. Vandalismo	Qual o grau de resistência ao vandalismo? Que tipo de proteções apresenta contra o vandalismo?
10. Intrusão física	Que tipo de proteção o dispositivo possui contra tentativas de intrusão fraudulenta, como abertura indevida? O hardware onde se encontra o dispositivo de captura é lacrado? Qual tipo de criptografia utilizada na comunicação com este hardware? O dispositivo possui alguma certificação, como por exemplo FIPS?
11. Longevidade perante o ambiente	Qual a resistência do equipamento contra o desgaste provocado pela variação das condições ambientais, como temperatura, umidade, luminosidade, salinidade, produtos de limpeza/abrasivos, etc ?
12. Log	A solução gera e armazena dados de auditoria? Possui memória não volátil? Possui relógio interno?
13. Manutenção	Quais as recomendações, exigências e restrições relacionadas à manutenção e conservação do dispositivo?
14. Resistência a fraudes	O dispositivo está preparado para resistir a que tipos de ataques/fraudes? Descreva os mecanismos implementados para proteção de cada um?
15. Material	Qual o material do envoltório do equipamento? Existe flexibilidade para adoção de outro material para a caixa envoltória do equipamento, diferente do original? O material utilizado está aderente as normas de preservação ambiental.
16. Garantia para pintura	Qual o tempo de garantia dado pelo fabricante para a pintura e para o acabamento do equipamento em situação de uso normal?
17. Manutenção de pintura	A manutenção da pintura e/ou acabamento do equipamento pode ser feita no local onde instalado? Em caso negativo, existem empresas autorizadas para a execução de tais serviços?

	Solução - Processo de registro
18. Processo de registro	Descreva as etapas do processo de registro do perfil biométrico, desde a aquisição do exemplar, extração das características, criação perfil biométrico, transformações (compactação, cifragem, etc.) e armazenamento.
19. Atualização do perfil	Em que situações há necessidade de refazer a captura posteriormente? Após quanto tempo?
20. Exemplar adquirido	Quais as características do exemplar (imagem, voz, etc.) adquirido, em termos de tamanho (bytes) e resolução?
21. Perfil extraído	Qual o tamanho do perfil biométrico extraído (bytes)?
22. Perfil armazenado	Qual o tamanho do perfil biométrico armazenado (bytes), após sofrer eventuais transformações, como compactação, cifragem, etc.?
23. Armazenamento	O perfil biométrico pode ser armazenado alternativamente em outros locais, como no dispositivo biométrico, em servidor externo (mainframe, HSM, etc) ou em smartcards? Existe possibilidade de esse armazenamento ser realizado em um módulo criptográfico?
24. Smart card	Caso o perfil biométrico possa ser armazenado em smartcard, quais são os requisitos do cartão, em termos de armazenamento, velocidade da CPU e sistema operacional?
25. Interoperabilidade	O perfil biométrico segue algum padrão internacional de armazenamento? Qual?
26. Interoperabilidade	O formato de armazenamento do perfil biométrico é público/aberto?
27. Interoperabilidade	Existe alguma possibilidade do perfil biométrico gerado ser validado por outra solução?
28. Interoperabilidade	Cite exemplos de utilização do padrão por outra solução.
29. Interoperabilidade	O algoritmo de geração é aberto/público?
30. Perfil biométrico cancelável	Existe possibilidade de armazenamento do perfil biométrico "transformado", de modo a proporcionar cancelamento/revogação em caso de vazamento do perfil biométrico armazenado no banco de dados?
31. Exceções	Pode haver situações em que o usuário não seja cadastrado e/ou autenticado, mesmo seguindo todos os procedimentos de utilização do dispositivo? Por exemplo, no caso de queimaduras, calos, abrasão, catarata, cegueira, utilização de óculos e lentes de contato, sudorese, salinidade, etc.? Quais as situações em que o usuário não poderá se cadastrar / autenticar....
32. Retorno	O equipamento fornece informações de retorno sobre a qualidade do exemplar colhido?
33. Posicionamento	Quais as exigências em relação à distância e posicionamento adequados do usuário para proporcionar a aquisição adequada do exemplar biométrico? Exige contato físico?
	Solução - Processo de autenticação
34. Tempo de resposta	Quais os tempos de resposta para os seguintes passos: Aquisição do exemplar, obtenção do perfil biométrico e comparação dos perfil biométricos em processamento local?

35. Processo	Como funciona o processo de comparação? O algoritmo de validação é aberto/público?
36. Local	O processo de comparação pode ser efetuado no dispositivo, em servidor externo (mainframe, HSM, etc) ou em smart card?
37. Porte para mainframe	O módulo de comparação é portátil para o ambiente de mainframe? De que forma será disponibilizado o módulo de comparação para os bancos, caso a comparação seja efetuada no mainframe? Existe possibilidade de essa comparação ser executada em um módulo criptográfico?
38. Código-fonte	O código-fonte dos módulos de aquisição, extração e comparação do perfil biométrico, pode ser confiado para os bancos, como depositário, mediante contrato de sigilo?
39. Calibração	O limiar de comparação pode ser configurado, para tornar o processo mais rigoroso ou mais permissivo? É possível configurar o limiar de comparação via API? Essa calibração pode ser adaptada ao ambiente?
40. Precisão	Qual é a estimativa das taxas de precisão? Quais os pares de taxas para o modo permissivo, modo padrão (EER) e modo rigoroso? As taxas de FAR e FRR foram certificadas por alguma instituição? Foram utilizados usuários reais para estimativa das taxas de precisão?
Solução – Integração com a aplicação	
41. API	A arquitetura de implementação da sua solução é estruturada em camadas que facilitem a integração com a aplicação do terminal de auto-atendimento dos bancos, com provimento de módulos de software que operem em regime de interface para aplicação (API), para controle do dispositivo, oferecendo inclusive capacidade de monitoramento on-line através de sistemas próprios dos bancos?
42. SO's	As APIs podem ser implementadas em quais sistemas operacionais? Detalhar versões, distribuições suportadas, Service Packs, linguagem, etc
43. BioAPI	A sua solução é compatível com a BioAPI 2.0 (ISO 19784)?
44. SDK	Para quais ambientes e sistemas operacionais são fornecidos SDK? Em quais linguagens?
45. Atualização	Quais são as formas de atualização de firmware? Quais são as formas de atualização das versões do software?
46. Hardware	Existem casos de adaptação do hardware em terminais de Auto-Atendimento? Detalhar em quais equipamentos (tipo, fabricante, etc) estas adaptações foram realizadas. Existem empresas certificadas a fazer esse trabalho no Brasil?
47. Hardware	O dispositivo é entregue em módulo físico único? Enumere os componentes de hardware da sua solução (conectores, cabeamento, etc.) necessários para o funcionamento em conjunto com o terminal de auto-atendimento.
48. Software	Quais são os componentes de software da sua solução? Detalhar a arquitetura de implementação.
49. Conexão	Como é feita a conexão do dispositivo, na camada física, com o terminal de auto-atendimento?
50. Privacidade	Como é garantida a comunicação segura dos dados entre o dispositivo, o local de armazenamento do perfil e o local de processamento da comparação?
51. Administração	Como a solução permite autenticação e acesso para manutenção/configuração do equipamento pelo administrador?

52. Autenticação do dispositivo	Qual é a possibilidade de autenticação do dispositivo junto ao sistema do Banco, na fase de inicialização e em outros momentos do ciclo de funcionamento do dispositivo?
53. Vinculação	É possível vincular o dispositivo para que somente funcione em um determinado equipamento? Em caso positivo, como? É possível posteriormente desvincular para instalar em outro equipamento?
54. Testes	O dispositivo pode ser entregue para testes em laboratório, em regime de comodato, com todas as funcionalidades necessárias? Fica ressalvado que quaisquer resultados de testes não representam nenhuma homologação ou certificação por parte da FEBRABAN.
Solução – Integração com o mercado	
55. Base instalada	Quantos ATMs existem instalados com a sua solução? Onde?
56. Utilização	Que outras empresas no mundo utilizam o dispositivo em questão em outros equipamentos?
57. Custo	Qual a estimativa do custo total da sua solução? Este custo é escalável? Como?
58. Custo	Qual o custo de reposição?
59. Custo	Existem outros custos como, por exemplo, de manutenção e consultoria?
60. Fornecimento	Sua empresa é a única fornecedora da solução?
61. Representação	A empresa possui representantes/parceiros que forneçam a sua solução no Brasil?
62. Logística	Qual a estrutura existente para fabricação, entrega, instalação, suporte técnico e manutenção, a nível nacional? Qual a capacidade produtiva mensal da solução?
63. Parceria com integradores	A empresa possui representantes/parceiros que integrem a sua solução com ATMs?

Terminologia básica

Posse, conhecimento e biometria

As credenciais apresentadas para autenticação podem ser de três tipos: (1) posse - Qualquer detentor da posse de um objeto é capaz de utilizar o recurso; (2) conhecimento - Indivíduos possuidores de certo conhecimento são elegíveis para utilizar um recurso; e (3) biometria - Os traços das pessoas podem ser medidos e computados na forma de um identificador biométrico único, difícil de compartilhar, roubar, forjar e de ser alterado.

Assim, a autenticação baseada em características biométricas vem despertando grande interesse de fabricantes, desenvolvedores, empresas e usuários finais. Nos parágrafos a seguir, é proposto um conjunto de nomes para tornar mais efetiva a comunicação entre os representantes destas entidades.

Processo de registro e perfil biométrico (perfil biométrico)

Seja qual for a característica biométrica utilizada, ela pode ser enquadrada em um sistema biométrico. Um modelo conceitual simples de um sistema biométrico (ver Figura) leva em

consideração os dados e processos básicos comuns a qualquer sistema biométrico. O usuário é previamente registrado e seu perfil biométrico fica armazenado (perfil biométrico).

Processo de aquisição e exemplar

Quando da utilização posterior do sistema, o processo de aquisição coleta os dados biométricos apresentados novamente pelo usuário, obtendo um exemplar. Características particulares dos dados são extraídas para comparação com o perfil armazenado. O processo de comparação decide se os dados apresentados (exemplar) são suficientemente similares ao perfil registrado.

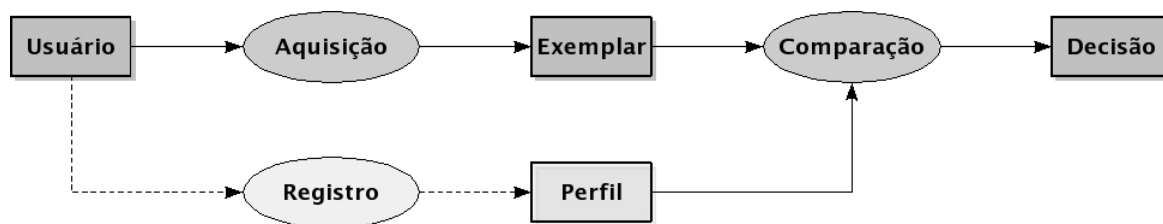


Figura - Modelo simples de um sistema biométrico.

Processo de comparação, escore, limiar e decisão

O processo de comparação, ou match, verifica qual é o grau de similaridade entre as características extraídas do exemplar apresentado pelo usuário e o perfil armazenado previamente. Este processo fornece um escore representativo da similaridade entre os dois conjuntos de dados. Caso a similaridade seja superior a certo limite previamente determinado, conhecido como limiar, ou threshold, a decisão é aceitar o usuário, ou seja, uma autenticação válida. Caso a similaridade seja inferior ao limiar, a decisão é não aceitar o usuário, e então temos um usuário não autenticado.

Modos de autenticação

Os sistemas biométricos são usados para a autenticação de pessoas. Nestes sistemas, existem dois modos de autenticação: a verificação e a identificação.

Na verificação, a característica biométrica é apresentada pelo usuário juntamente com uma identidade alegada, usualmente por meio da digitação de um código de identificação. Esta abordagem de autenticação é dita uma busca 1:1, ou busca fechada, em um banco de dados de perfis biométricos. O princípio da verificação está fundamentado na resposta à questão: “O usuário é quem alega ser?”.

Na identificação, o usuário fornece apenas sua característica biométrica, competindo ao sistema “identificar o usuário”. Esta abordagem de autenticação é dita uma busca 1:N, ou busca aberta, em um banco de dados de perfis biométricos. O sistema busca todos os registros do banco de dados e retorna uma lista de registros com características suficientemente similares à característica biométrica apresentada. A lista retornada pode ser refinada posteriormente por comparação adicional, biometria adicional ou intervenção humana. Basicamente, a identificação consiste em responder à questão: “Quem é o usuário?”.

Erros

Todas as tecnologias biométricas estão sujeitas a erros estatísticos, como falsa aceitação de impostores e falsa rejeição de usuários genuínos. As taxas de falsa aceitação (FAR) e falsa rejeição (FRR) são inversamente relacionadas, de modo que o ajuste de um sistema biométrico para reduzir uma delas, produz automaticamente um aumento na outra. Rigorosamente falando, as taxas FAR e FRR não são “ajustadas” por um administrador de sistema. Ao invés disto, o administrador ajusta um “limiar” de comparação, e o ajuste deste limiar produz impacto em ambas as taxas simultaneamente, melhorando uma delas, mas piorando a outra (ver Figura).

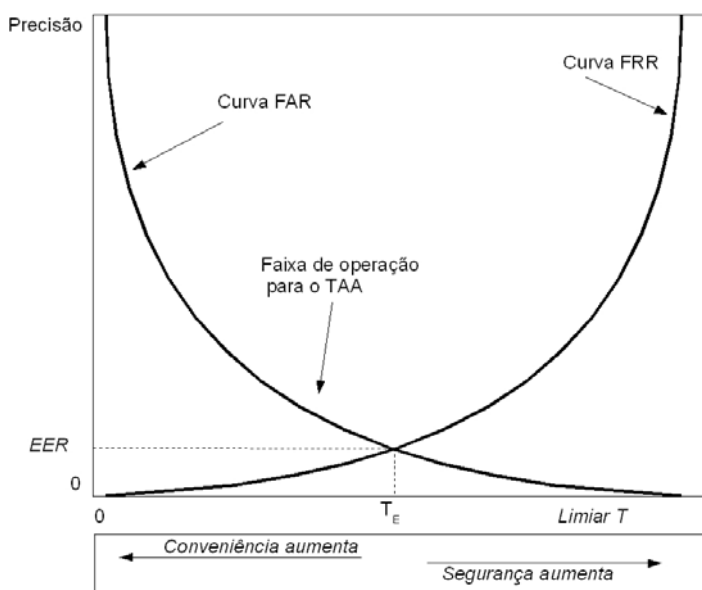


Figura - Curva representativa das taxas de erros de sistemas biométricos

Devido ao relacionamento entre as duas taxas de erro, a precisão de um sistema somente faz sentido quando é informado o par de taxas de erro. Ou seja, qualquer sistema pode alegar uma taxa de falsa aceitação de 0% simplesmente rejeitando toda e qualquer tentativa de utilização (inclusive as válidas). Similarmente, qualquer sistema pode alegar uma taxa de falsa rejeição de 0%, simplesmente aceitando toda e qualquer tentativa (inclusive as inválidas). Assim, um sistema biométrico deve ter sua precisão avaliada por meio da informação do par de taxas, que constitui seu ponto de operação.

Um ponto de operação interessante é o ponto onde as taxas são iguais, conhecido como EER, ou ponto de cruzamento. Por meio desta taxa EER, pode-se ter um vislumbre da precisão do sistema em consideração. No entanto, a política de decisão do sistema é ajustada de acordo com as necessidades da organização que vai utilizá-lo.