Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Estudo, Análise, Modelagem e Projeto de Serviços e de Modelos Canônicos de Dados

Data de Emissão:

02/06/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
06/03/2015	0.1	Versão inicial.
10/03/2015	0.2	Incluído para detalhamento o capítulo "Arquitetura de Referência"
12/04/2015	0.3	Versão preliminar para avaliação
26/05/2015	0.4	Ajuste do documento para análise e homologação.
02/06/2015	0.5	Revisão de texto e forma.

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1 INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de sete de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa aperfeiçoar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto

que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

Resultante de um subconjunto das atividades previstas para inicialização da cooperação MJ/SE e FUB/CDT, o presente documento contempla os resultados da realização do processo de análise e modelagem dos serviços candidatos para serem implementados como referencial a ser posta em teste na forma de Prova de Conceito visando obter alguns indicativos de desempenho e modelos que podem ser utilizados.

2 REFERENCIAL TEÓRICO

O presente documento tem a intenção de apresentar o escopo inicial de serviços candidatos para uso em toda extensão do sistema RIC. Como resultado de atividades de análise e modelagem orientada a serviços, as quais atendem os requisitos atuais de interoperabilidade, de execução em ambientes de nuvens e de escalabilidade, os princípios de sua metodologia se baseiam fortemente na Arquitetura Orientada a Serviços - SOA, tal qual exposta nos modelos discutidos no referencial de Erl (2005). De Thomas Erl (Erl, Service-Oriented Architecture: Concepts, Technology & Design, 2005) define-se que:

> *"(...) na medida em que estão centrados em torno de serviços, os modelos organizacionais baseados em SOA associam as funcionalidades tecnológicas diretamente aos objetivos de negócios, num encadeamento de processos integrados".*

2.1 RT Inventário Preliminar de Serviços para o RIC

Muito da discussão das vantagens do uso de SOA, de seus conceitos e princípios, e dos elementos centrais dessa arquitetura são apresentados no RT Inventário Preliminar de Serviços para o RIC, sendo condição essencial sua leitura para entendimento do que é tratado neste documento.

Desse Relatório Técnico extraímos apenas o seguinte entendimento, a saber.

> "(...) Um serviço SOA é a unidade lógica projetada segundo os princípios da orientação a serviços. São estruturas sistêmicas que possuem um contrato formal com declaração de suas entradas, saídas, possíveis exceções, funcionamento, versão, etc. Um serviço representa uma funcionalidade do negócio, que tem por objetivo a troca de dados entre fornecedor e consumidor; estes, podem ser outros blocos sistêmicos ou interfaces como o usuário".
>
> "(...) Os serviços realizam atividades sistêmicas a partir de capacidades / operações, e são essas capacidades que são chamadas quando da execução de uma atividade. Como exemplo, o serviço de Validação tem uma capacidade chamada autenticar, que recebe uma mensagem e retorna uma resposta a essa. Capacidades / operações de serviço encontram similaridade com as funções e procedimentos (*functions e procedures*) no desenvolvimento de sistemas

tradicionais / monolíticos".

"(...) Serviços tem como característica essencial seus modelos. Modelos de serviços são classificações estabelecidas para criar camadas lógicas de abstração que organizam um inventário de serviços. Modelos de serviço provêm meios de atribuir uma etiqueta permanente a serviços que representam seu propósito e função geral. Um modelo de serviço essencialmente estabelece um contexto funcional base para um serviço que irá então ser refinado durante o processo de modelagem de serviço".

"(...) Assim, as lógicas expressas por serviços - que definem seu modelo - podem ser classificadas como lógica de negócio quando ela é derivada de modelos de análise e especificações de negócio. Exemplos desse tipo de documentos incluem fluxo de trabalho (*workflow*) ou definições de processos de negócio, especificações BPM, ontologias, taxonomias, modelos lógicos de dados, diagramas de entidades de negócio e uma variedade de outros documentos relacionados com a análise negocial, análise de dados e arquitetura da informação. Outras partes da lógica de processamento que não são relacionadas ou derivadas da lógica de negócio podem ser classificadas como lógica utilitária. Esse tipo de lógica está relacionado a diversas funções de processamento disponíveis como recursos tecnológicos que apoiam a construção de soluções tecnológicas automatizadas".

Nesse sentido, são considerados cinco modelos comuns de serviço (Figura 2.1):

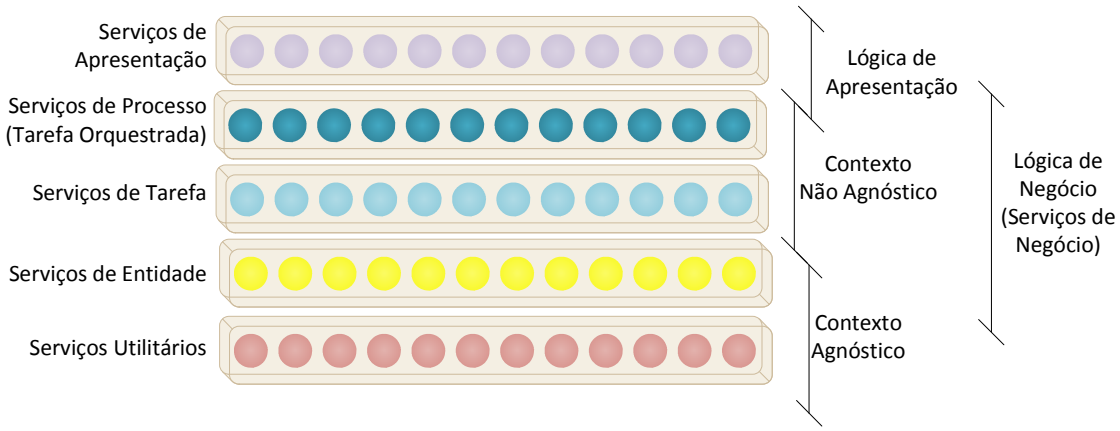


Figura 2.1: Modelos de Serviços

- Serviços de Apresentação: são *softwares* que realizam interfaces de usuário compartilháveis e extensíveis que podem ser invocados por outros elementos (i.e. serviços ou plataforma de SOA) de uma solução SOA. Estes serviços estão associados com a camada de apresentação do modelo lógico desta arquitetura de referência. Uma lógica residindo na camada de apresentação pode não precisar, de fato, ser encapsulada por um serviço.

- Serviços de Processos (Tarefas Orquestradas): são os que encapsulam lógica de processos de negócio pai. Estes serviços estão associados com a camada de apresentação do modelo lógico desta arquitetura de referência.

- Serviços de Tarefa: são aqueles que encapsulam lógica de negócio específica de uma tarefa de negócio, frequentemente relacionada a atividades de processo (i.e. produz um resultado/saída). Se associada ao desenho de um fluxo de processo em BPM, as atividades (quadrados arredondados) são capacidades de serviços de tarefa, enquanto todo um processo em uma pista (*lane*) é um serviço de processo (tarefa orquestrada).

- Serviços de Entidade: são aqueles cujo contexto é derivado de uma entidade de negócio específica, por exemplo, usuário, profissional, estabelecimento, e ou de um grupo de entidades de negócio relacionadas. As capacidades / operações de serviços de entidade provêm funcionalidades centradas em torno do processamento do conjunto de informações associado com a entidade de negócio.

- Serviços Utilitários: provêm funcionalidade que endereça interesses múltiplos, enquanto mantêm um escopo funcional não negocial. Frequentemente, encapsulam recursos corporativos, tais como sistemas legados e bases de dados, e os expõem em contextos únicos. Residem na parte de baixo de hierarquias de composição, onde são compostos por serviços de tarefa e de entidades.

A Figura 2.2 ilustra a relação entre os modelos de serviço definidos na arquitetura e os tipos de lógica que compõem cada contexto respectivo.

	Lógica de Apresentação	Lógica Negocial	Lógica Utilitária	Lógica Agnóstica	Lógica Não-Agnóstica
Serviços de Apresentação					
Serviços de Processo					
Serviços de Tarefa					
Serviços de Entidade					
Serviços Utilitários					

Figura 2.2: Modelos de Serviços *vs* Tipo de Lógica

Outros modelos especializados de serviço que podem ser definidos, conforme dado a seguir:

- Serviços de Persistência e Adaptadores de Banco de Dados (Utilitários): provêm acesso direto a recursos de persistência de dados, usando estruturas de dados nativas.
- Serviços de Sistemas Legados (Utilitários): encapsulam lógica de sistemas legados, expondo-a como serviço.
- Serviços de ETL (Utilitários): provêm funções de processamento de múltiplas transações/registros, em lote (*batch*).
- Serviços de Replicação de Dados (Utilitários): provêm lógica de replicação de dados entre aplicações diferentes. Podem operar tanto em modo síncrono quanto em modo assíncrono, dependendo da arquitetura de replicação adotada.
- Serviços de Gerenciamento do Modelo Mestre de Dados (MDM) (Utilitários): provêm acesso a lógica de MDM corporativa.
- Serviços de Convergência de Interatividade (Utilitário): provêm acesso a recursos de comunicação e interatividade, tais como telefonia, *e-mail*, *chat*, videoconferência, entre outros.

- Serviços Canônicos (Entidade): provêm acesso a bases de dados corporativas normalizadas, através de modelos de representação de informações e seus relacionamentos consistentes e padronizados.
- Serviços de Regras de Negócio (Tarefa): provêm centralização de regras de negócio.
- Serviços de Monitoramento de Negócio (Tarefa): provêm lógica de monitoramento de processos, normalmente realizada em tempo real (BAM).
- Serviços de Apoio a Decisão (Tarefa): provêm acesso a dados analíticos (lógica de *Business Intelligence – BI*).

2.2 RT Estudo sobre Soluções de *Message Queue* / Barramento de Serviços Corporativos

Para o estabelecimento de uma infraestrutura aderente a Arquitetura Orientada a Serviços (SOA) e com condições de suportar o esperado volume de acesso massivo, contínuo e distribuído baseado em serviços web como idealizado para o RIC, há de se conhecer ao mínimo o escopo do RIC, os arquétipos necessários e, principalmente, os serviços essenciais que devam ser providos pela infraestrutura do mesmo.Soluções baseadas em SOA são tipicamente sistemas cooperativos abertos nas quais, novas entidades podem dinamicamente passar a compor o sistema, evoluírem, ou mesmo, deixarem de existir.

Além disto, em virtude da distribuição e do uso comum de um *middleware* orientado a mensagens (e interoperável), existe a possibilidade de que sistemas baseados em SOA sejam suportados por ambientes heterogêneos distribuídos geograficamente, isto é, os componentes dos sistemas (serviços) podem estar sendo executados em máquinas distintas, fisicamente distantes e heterogêneas, precisando apenas se comunicar por troca de mensagens.

Assim, no que se trata do referencial teórico já documentado, da realização de diversos princípios de infraestrutura aderentes a realização de um projeto de SOA, também se faz necessário o conhecimento do componente tecnológico essencial nas implementações baseadas nessa arquitetura: o Barramento de Serviços Corporativos - ESB. Assim, também é leitura essencial o RT Estudo sobre Soluções de *Message Queue* / Barramento de Serviços Corporativos.

2.3 Agrupamento dos Serviços Candidatos e suas Capacidades

A Figura 2.3 ilustra uma representação visual que define certo agrupamento/ classificação para os serviços do RIC com os requisitos eles realizam.

Figura 2.3 Representação dos Grupos de Serviços e os Requisitos Cumpridos

Em um detalhamento mais específico temos para esses grupos as informações descritas a seguir.

- **Serviços de Autenticação (Validação e Identificação):** acesso com mais baixa latência, pouco recurso de composição de serviços, alta escalabilidade (incluindo escalabilidade geográfica) e bases de dados de alto desempenho, se possível, usando SGBD em memória (*in-memory*).
- **Serviços de Federação (Identidade Federada):** acesso através de chaves que garantam a portabilidade de credenciais na execução de processos dentro do ecossistema RIC.
- **Serviços de Registro (Criação da chave primária):** composição de serviços entre os ABIS e a criação da chave única do RIC com suporte a redistribuição nas bases de dados localizadas.
- **Serviços de Cadastramento (Cadastro de dados básicos e documentos):** modelo de média latência, porém síncrono.

- **Serviços de Informação (Requisição-Resposta a solicitações de terceiros):** serviços síncronos de informação.
- **Serviços de Integração (Requisição-Resposta a requisições do RIC):** modelo síncrono de solicitações do RIC para serviços de terceiros no modelo requisição-resposta; com fortes requisitos de tolerância às falhas.
- **Serviços de Comunicação (Mensageria Direcionado por Eventos):** modelo assíncrono baseado em princípios de padrões de mensageria *publish-subscribe*.
- **Serviços de Atendimento (Processo de Agendamento):** operações de CRUD tanto para o processo de agendamento ou outros atendimentos aos cidadãos.
- **Serviços de Operacionalização (Processo de Emissão de Documentos RIC):** operações de CRUD para informação aos prestadores de serviços de emissão do documento referente ao RIC.
- **Serviços de Auditoria (Notificar Log, Auditoria e "Problemas Graves"):** mensageria assíncrona – notificação para bases de dados de auditoria do registro do RIC bem como de acesso ao RIC.
- **Serviços de Sincronismo (Sincronizar Bases Geodistribuídas):** modelo assíncrono de garantia de sincronia entre a base centralizada e os elementos distribuídos do modelo.
- **Serviços Analíticos (*Business Intelligence - BI*):** utiliza-se de relatórios pré-formatados e cubos multidimensionais para consultas *ad-hoc* e análise multidimensional.

3 ANÁLISE REFERENCIAL DE PADRÕES

3.1 Introdução

Em 2012, a OASIS abriu para discussões o documento *"Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0"*, datado de maio de 2012, que apresenta uma especificação de um perfil SOAP para implementar as operações abstratas especificadas no INCITS 442.

Este documento inicia-se pela exposição dos padrões que definem o entendimento do comitê técnico da OASIS das necessidades estruturais para que se possa prover um mecanismo cliente/servidor interoperável baseado no protocolo SOAP (contratos - WSDL e mensageria XML baseada em esquema XML - XSD), contextualizando sua proposta aos esforços colaborativos à época entre governo e a indústria privada na especificação de uma plataforma de aplicação consistente e independente de interesses organizacionais.

Assim, para dar base ao uso de definições comuns, o documento já elenca no seu início um conjunto de referência normativas e não normativas para suportar recomendações existente dentro do seu escopo (e.g. a ISO/IEC 19785-1:2006, a especificação de *framework* de formato de troca de dados biométricos da ISO).

3.2 Terminologia Utilizada

Em adição aos termos correlatos em tecnologia Web (HTML, HTTP, HTTPS, URI, XML, URL, TSL) e à Arquitetura Orientada a Serviços - SOA (SOAP, WSDL, XSD, WS-*, *implementation*, *endpoint*), alguns termos específicos são apontados pelo documento que são necessários para todo entendimento da análise realizada a seguir. Assim é necessário reapontá-los e referenciá-los, a saber.

- BIAS - *Biometric Identity Assurance Services*: serviços propostos (capacidades de serviços, grifo do autor) para atender aos processos elementares de garantia de identificação biométrica.
- BIR - *Biometric Information Record*: modelo que agrupa todos os dados necessários para registro das informações biométricas.
- CBEFF - *Common Biometric Exchange Formats Framework*: elementos de dados e formatos específicos de BIR, especificados na ISO/IEC 19785-1.

Dada a importância no contexto das capacidades primárias do RIC, ainda é necessário o entendimento do que se descreve como Operações Agregadas (*Aggregate Operations*), que reportam aos dois requisitos básicos que o perfil de serviços referendado atende: de Cadastramento (*ENROLL*) e de Autenticação (*IDENTIFY*).

- **Cadastramento (*Enroll*)**: a operação de cadastramento adiciona um novo elemento ao modelo centrado na unicidade de identificação. Isto pode ser realizado de diversas maneiras, de acordo com os requisitos e / ou os recursos do sistema. Durante o registro, a informação biométrica de um indivíduo é captada e armazenada. Corresponde as etapas de aquisição e de correspondência (*template matching*) que é descrita nos documentos como etapa de deduplicação.

  Se a operação de Identificação é implementado como um serviço síncrono, o sistema processa imediatamente o pedido e devolve os resultados da base de dados. Se a operação é implementada como um serviço assíncrono, o sistema de execução retorna um *token* de protocolo no parâmetro de retorno de dados, o que é uma indicação de que o pedido está sendo tratado de forma assíncrona. Em geral, é implementado de forma assíncrona através de processos de deduplicação.

  O conceito de deduplicação refere-se ao processo de examinar, durante o procedimento de cadastramento, se a amostra biométrica que está sendo cadastrada tem alguma amostra correspondente em todo o banco de dados já existente. Desta forma, a amostra e comparada as "N" amostras já cadastradas, uma a uma. Se existe alguma amostra correspondente, o indivíduo não é cadastrado, e, portanto, não recebe uma nova identidade a fim de evitar uma entrada duplicada. Caso não exista amostra correspondente, o usuário e cadastrado de forma correta e um número único e associado a amostra apresentada pelo individuo (Decann, 2013).

  O processo de deduplicação é necessário para garantir que todos os indivíduos da população tenham apenas um único número no banco de dados. Por exemplo, uma entrada duplicada pode ser criada intencionalmente por um impostor para futuramente fraudar o sistema e obter algum benefício utilizando a identidade de outro indivíduo. O processo de deduplicação vem ganhando atenção nos últimos

anos, devido particularmente a programas de identificação civil de grande escala como o caso da Índia, México e Indonésia, em que enormes bases de dados precisam garantir a unicidade dos indivíduos cadastrados.

A deduplicação também pode ser considerada um processo de identificação, em que e feita uma comparação 1:N. Entretanto, para cada indivíduo que está sendo cadastrado e realizada uma comparação, o que exige alto poder de processamento do sistema. Como exemplo da complexidade dessa operação, a Índia cadastra, diariamente, 1 milhão de indivíduos, os quais são comparados com os 650 milhões já cadastrados, gerando mais de 500 trilhões de comparações por dia (Portal UIDAI).

- **Autenticação (*Identify*)**: a operação de autenticação desempenha uma função de identificação de um elemento de acordo com requisitos e / ou recursos do sistema. Se a operação é implementada como um serviço síncrono, o sistema processa imediatamente o pedido e devolve os resultados de acordo com a base de dados. Se a operação é implementada como um serviço assíncrono, o sistema retorna um *token* de protocolo no parâmetro de retorno de dados, que é uma indicação de que o pedido está a ser tratado de forma assíncrona. Neste caso, existe uma operação (no caso em análise, a capacidade de serviços *GetIdentifyResults*, que será especificada no decorrer deste documento), a qual é usada para avaliar os resultados do pedido de autenticação para tratar a situação assíncrona.

3.3 Análise do Referencial

Inicialmente é necessário que se aponte que o modelo utilizado para o suporte a serviços pode ser implementado sob duas perspectivas: **centrado na pessoa (*person-centric*)** no qual as informações são sobrepostas para cada pessoa, ou em suas **situações (*encounter-centric*)**, no qual o registro de situações de uma pessoa é agrupado em galerias, segundo um único identificador.

O entendimento do modelo centrado na pessoa é que ele se baseia em princípios de substituição, no qual a última informação/registro é considerada predominante (por um *timestamp*), porém o cidadão é único. No modelo baseado em situações, registros são isolados em situações (*encounters*) que podem ser agrupados pelo mesmo identificador (*subject id*).

Esse tipo de conhecimento é importante antes da análise da proposta apresentada pela OASIS. A Figura 3.1 ilustra esse entendimento.

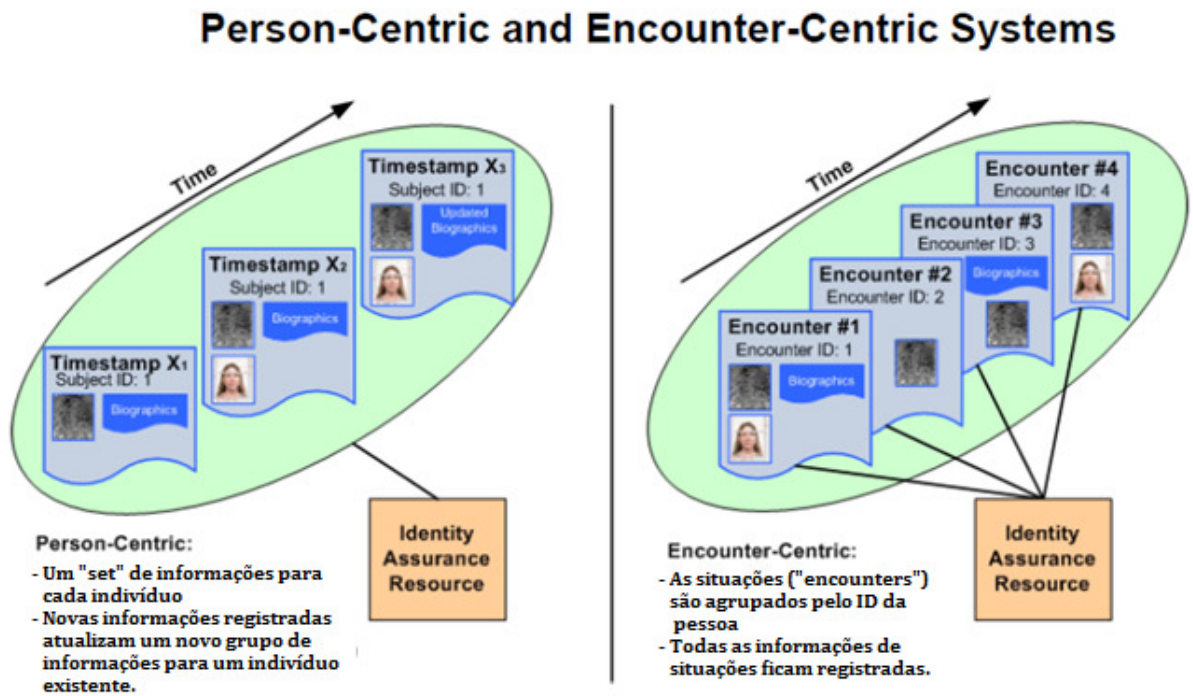


Figura 3.1 - Modelo Person-Centric vs. Encounter-Centric.

Em continuidade da análise da proposta contida, no que se refere a arquitetura apresentada, o documento citado sugere que a definição é essencial para o detalhamento

do provimento/consumo de serviços e, principalmente, nos princípios que irão governar o projeto do armazenamento de dados no servidor.

No que se refere ao acesso a esse modelo de provimento/consumo, esses são estabelecidos no contexto do modelo do BIAS, como ilustrado na Figura 3.2:

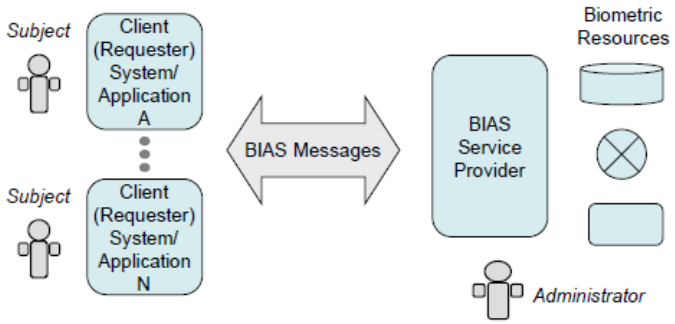


Figura 3.2 - Contexto do BIAS

Neste ponto cabe relembrar o modelo arquitetural de SOA em seu modelo de Baixo Acoplamento que provê uma interface (Contrato de Serviços - WSDL) que contém a lista de capacidades (operações) ofertadas independente do que está codificado. Assim, código (*software* compilado) pode ter diversas funcionalidades, mas que o acessa só pode acessar a determinados serviços ofertados (o contrato tem um "ponteiro para" a funcionalidade). Isto permite uma manutenção mais ágil do programa sem que se imponha nenhuma mudança nos sistemas que usam o serviço (o contrato ofertado).

Em continuidade, na interpretação da Figura 3.3 a seguir e de seus textos associados, observa-se que a OASIS já sugere as pré-existência de determinados serviços complexos (serviços de tarefa que realizam diversas funcionalidades em sequencia - composição de serviços) atendidos no âmbito sua interface de serviços que são providos como componentes através dos ditos terminais (o "ponteiro para" existentes nos contratos de serviços) que encapsulam lógicas de acesso a recursos de infraestrutura de dados e de um *framework* de biometria (*BioAPI Framework*) através de adaptadores, para permitir a flexibilidade de resposta as funcionalidades pelas diversas API existentes e desenvolvidas pelos fornecedores do mercado.

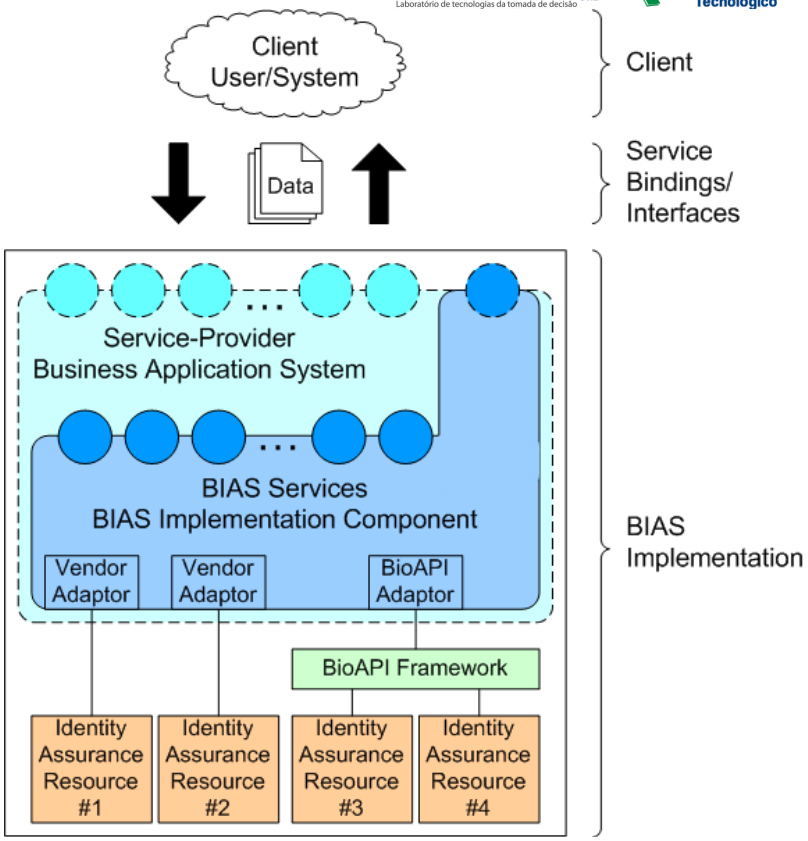


Figura 3.3. Arquitetura Básica sugerida pela OASIS para o BIAS

3.4 Padrões Revisados

No que se refere à manutenção de padrões de interoperabilidade mundial, elencamos a lista de padrões conhecidos que servem de base para diversas definições - entre elas a de conteúdo de mensagens a serem trocadas entre aplicações clientes e os serviços do RIC, a saber.

3.4.1 Padrões de Interface Técnica para Processos Biométricos

- ANSI INCITS 358-2002 [2007] - *The BioAPI Specification*: especifica o API e a interface de provimento de serviços biométricos para uma tecnologia biométrica padrão. Esta especificação está além da definição dos requisitos de segurança para aplicações biométricas e prestadores de serviços, embora algumas informações relacionadas estejam incluídas para explicação de como a API destina-se a apoiar as boas práticas de segurança. O BioAPI se destina a fornecer um genérico modelo de autenticação biométrica de alto nível; indiferente de

qualquer forma de tecnologia biométrica. A norma abrange as funções básicas de cadastro, verificação e identificação, e inclui uma interface de banco de dados para permitir que um prestador de serviços biométricos (BSP) possa gerenciar a Identificação para um melhor desempenho para toda uma população de pessoas. Ele também fornece primitivas que permitem que ao aplicativo gerencie a captura de amostras em um cliente, seu cadastro, sua verificação e identificação junto a um servidor de serviços biométricos.

- INCITS 358:2002 *AMENDMENT* 1: 2007 - *BioAPI Specification* – Emenda 1: *Support for Biometric Fusion*: provê os conceitos básicos para suporte ao processo de "fusão" na biometria.
- A edição apontada do INCITS 358 (BioAPI 1.1) não fornece nenhum suporte direto para a fusão biométrica. Além disso, o uso de FARs na representação de pontuações correspondentes não é adequada no geral para a realização de fusão baseada no nível de pontuação (apesar de permitir que algumas formas limitadas de fusão). Esta alteração adiciona suporte para a fusão biométrica. Ela estende a API e a SPI de BioAPI especificando novas funções e novos valores para os tipos de dados existentes.
- ANSI INCITS 398-2008 (Revisão da ANSI INCITS 398-2005) - *Common Biometric Exchange Formats Framework* (CBEFF): especifica um conjunto comum de elementos de dados necessários para suportar as múltiplas tecnologias biométricas e para promover a interoperabilidade dos programas e sistemas / aplicações biométricas. Assim, esta norma (em revisão da ANSI INCITS 398-2005) especifica um conjunto comum de elementos de dados necessários para suportar múltiplas tecnologias biométricas e promove, assim, a interoperabilidade dos programas e sistemas biométricos, permitindo a troca de dados biométricos. Estes dados comuns que podem ser colocados em um único arquivo, registro, ou objeto de dados usado para trocar informações biométricas entre diferentes componentes e aplicativos do sistema. Esta norma especifica os elementos de dados biométricos, que são montados em estruturas de dados que são definidos por especificações ou padrões de formato CBEFF. Resumindo, cada especificação de formato que está em conformidade com CBEFF, presentes em seu formato e como elementos de dados que são extraídos e transformados. Esta norma especifica dois formatos básicos padrões (consulte os anexos A e B da norma). Outros

padrões (anexos C a F) são especificações adicionais e externas a esta norma, a saber: (C) o formato BioAPI BIR.; (D) o formato The NIST PIV CBEFF - definido na NIST SP 800-76 de Fev 1, 2006; (E) a estrutura de dados lógicos do ICAO (*The ICAO Logical data* - LDS); e (F) o registro de tipo 99 (revisão da ANSI/NIST-ITL 1-2000 - ANSI/NIST-ITL 1-2007, "*Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information*"). O CBEFF não especifica o conteúdo ou formato dos dados biométricos reais contidos dentro de um registro de dados biométricos. As definições de proteção da privacidade dos indivíduos de divulgação e a utilização de dados biométricos descritos dentro dessa norma são consideradas inadequadas no âmbito geral, sendo revisto em outras normas correlatas.

- ANSI INCITS 434-2007 - *Tenprint Capture using BioAPI*: especifica requisitos para a utilização da ISO / IEC 19784-1 - a *BioAPI Specification* (também conhecido como BioAPI 2.0) - um padrão de interface de *software*, com a finalidade de realizar uma operação de captura Tenprint (dez digitais). Este inclui um ou mais dos seguintes procedimentos: (a) a identificação das funções BioAPI a serem utilizadas e o fim de serem chamadas; (B) a especificação de valores para os parâmetros de cada função; (C) a definição de eventos de interface (para uso com uma aplicação GUI controlada por sequência de eventos); (d) as especificações de interface do usuário para uso com um BSP (prestador de serviços biométrico) na suas interfaces; e (e) um exemplo chamando a sequências de entradas/saídas como exemplo.
- ANSI INCITS 442-2010 (Revisão da ANSI INCITS 442-2008) - *Biometric Identity Assurance Services* (BIAS): define serviços biométricos utilizados para a garantia da identidade, que são chamados (invocadas) através de uma estrutura baseada em serviços (composição de serviços). Ele se destina a fornecer um conjunto genérico de definições de dados biométricos e funções relacionadas para identificação, e permitem o acesso remoto a à serviços biométricos. A ligação destes serviços aos *frameworks* específicos não está incluída neste documento.

3.4.2 Padrões Metodológicos de Teste de Conformidade de Interfaces Técnicas para Processos Biométricos

- ANSI INCITS 429-2008 - *Conformance Testing Methodology for* ANSI INCITS 358-

2002 *of BioAPI Specification*: especifica os conceitos, estruturas, métodos de ensaio e os critérios a serem alcançados para garantir a conformidade de fornecedores de serviços biométricos segundo a especificação BioAPI ANSI INCITS 358- 2002. Ela define requisitos e orientações para especificar os conjuntos de testes de conformidade e métodos de ensaio relacionados de forma a medir a conformidade dos componentes do Provedor de Serviços Biométricos com a especificação BioAPI. Ainda, define os procedimentos a serem seguidos durante e após os testes de conformidade. A norma incide apenas sobre o conjunto crítico de funções/características da especificação BioAPI e outros requisitos, não tratando detalhes específicos ou requisitos adicionais.

3.4.3 Padrões de Formato de Troca de Dados/Mensagens para Processos Biométricos

- ANSI INCITS 377-2009 (Revisão da ANSI INCITS 377-2004) - *Finger Pattern Based Interchange Format*: especifica um formato de intercâmbio para a troca de dados de reconhecimento de impressões digitais baseadas em padrões. Descreve-se a conversão de uma imagem de impressão digital bruta para um padrão de recorte (*crop*) e para o padrão de "*down-sampled*", seguida pela definição da representação celular de imagem padrão de um dedo de forma a estabelecer os dados de transferência padrão para cada dedo.
- ANSI INCITS 378-2009 (Revisão da ANSI INCITS 378-2004) - *Finger Minutiae Format for Data Interchange*: esta norma é uma revisão da ANSI INCITS 378-2004 que define um método de representação de informações de impressão digital usando o conceito de minúcias. Ela define a colocação das minúcias sobre uma impressão digital, um formato de registro para conter os dados de pormenores, e extensões opcionais para contagem de cristas e de núcleos/deltas de informações.
- ANSI INCITS 379-2004 - *Iris Interchange Format*: descreve um formato para troca de informações sobre a imagem da íris. Ele contém uma definição de atributos, um formato de registro de dados, dos registros da amostra e os critérios de conformidade. Neste sentido, dois formatos alternativos para os dados de imagem da íris são descritos: um baseado em um sistema de coordenadas cartesianas e o outro num sistema de coordenadas polares.
- ANSI INCITS 381-2009 (Revisão da ANSI INCITS 381-2004) - *Finger Image Based*

Interchange Format: esta norma é uma revisão da ANSI INCITS 381-2004 que especifica um formato de intercâmbio para a troca de dados de reconhecimento de impressões digitais e da palma com base em imagens. Ele define o conteúdo, formato e unidades de medida para tais informações. Esta norma destina-se a essas aplicações de identificação e verificação que exigem o uso de dados de imagens *"in natura"* ou processadas, contendo informações detalhadas dos *pixels* (pontos nas imagens).

- ANSI INCITS 385-2004 - *Face Recognition Format for Data Interchange*: este padrão especifica as definições fotográficas (meio ambiente, a pose assunto, foco, etc.), entre elas propriedades e atributos da imagem digital fotográfica. Adicionalmente, define também um formato de intercâmbio de face para aplicações correspondentes, incluindo a identificação tanto humana como automatizada de reconhecimento facial.
- ANSI INCITS 395-2005 - *Biometric Data Interchange Format and Signature/Sign Data*: define um formato de intercâmbio de dados para dados de assinaturas para fins de inscrição biométrica, verificação ou identificação. A norma contém definições de dados brutos (imagens de assinaturas), dedados de séries temporais e das amostras, bem como aponta um formato de registro de dados para transmitir esses, incluindo dados estendidos ou proprietários.
- ANSI INCITS 396-2005 - *Hand Geometry Interchange Format*: especifica um formato de intercâmbio para a troca de dados de geometria de mão em formato de silhueta. Ele define o conteúdo, formato e unidades de medida para tais informações. Esta norma destina-se a essas aplicações de identificação e verificação que exigem o uso de um modelo interoperável de geometria da mão.
- ANSI INCITS 439-2008 - *Fusion Information Format for Data Interchange*: especifica formato interoperável para informações estatísticas do processo de fusão (FIFs) de forma modular. Esse formato registra informações de nível de pontuação de sistemas biométricos nos processos de fusão. A norma não define, nem descreve nenhuma forma de padronizar os processos de fusão.
- ANSI INCITS 456-2010 - *Speaker Recognition Format for Raw Data Interchange* (SIVR-1): esta norma define conceitos e especifica um formato de dados para a representação da voz humana em nível dos dados originais com a inclusão opcional de dados estendidos não-padronizados. Ela não aborda a manipulação

de dados que foram processados tais com os níveis de recursos ou de modelo de voz tratados. O formato dos dados é genérico, de forma que pode ser aplicado e utilizado num grande número de aplicações, no qual o tratamento automatizado de SIV (*"Speaker Identification Verification"*) é realizado. Não apresenta requisitos específicos de aplicativos, equipamentos ou características. Através de sua orientação XML, este padrão, no entanto, reflete o padrão VoiceXML no processamento da fala e outros padrões baseados em XML associados. Esta norma contém definições de termos relevantes, uma descrição da infraestrutura de reconhecimento de voz, um formato de dados para persistir os dados e informações de conformidade.

3.4.4 Padrões Metodológicos de Conformidade para teste dos Padrões de Formato de Troca de Dados/Mensagens para Processos Biométricos

- ANSI INCITS 423.1-2008 - *Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 1* (*Generalized Conformance Testing Methodology*): primeira parte de uma norma multiparte que especifica os conceitos, tipos de teste e metodologias de ensaio de conformidade para testar registros de intercâmbio de dados biométricos e/ou algoritmos de computador que criam registros de intercâmbio de dados biométricos. Os registros de intercâmbio de dados biométricos são especificados nos padrões de formato de intercâmbio de dados biométricos da INCITS. Esta parte define dois tipos (A e B) e três níveis (1, 2 e 3) de testes de conformidade, com uma descrição geral e metodologia para cada um. No caso dos dois primeiros níveis, existem muitos elementos de teste comum, e por isso a norma usa uma linguagem assertiva para especificar as afirmações de Nível 1 e 2 de teste. Esta norma não está preocupada com os testes de outras características dos produtos biométricos (tais como de requisitos não-funcionais) ou outros tipos de testes de produtos biométricos (ou seja, a aceitação, o desempenho, robustez, segurança).
- ANSI INCITS 423.2-2008 - *Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards - Part 2* (*Conformance testing Methodology* for ANSI INCITS 378-2004, *Finger Minutiae Format for Data Interchange*): segunda parte da norma ANSI INCITS 423 que especifica os testes necessários para garantir a aplicação dos padrões por um fornecedor de serviços que deverá estar de acordo com ANSI INCITS 378-2004. Para os efeitos desta

parte da ANSI INCITS 423, dos dois tipos (A e B) e três níveis (1,2 e 3) de teste de conformidade, tal como definido na norma ANSI INCITS 423 - Parte 1, apenas Tipo A e Níveis 1 e 2 estão dentro o âmbito desta parte do ANSI INCITS 423.

- ANSI INCITS 423.3-2009 - *Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 3* (*Conformance testing methodology for* INCITS 377-4 *Finger pattern data interchange format*): esta norma está preocupado com os ensaios de conformidade das implementações em conformidade com o formato de intercâmbio de dados para padrões de digitais (*Finger Pattern Data Interchange Format*) definida no INCITS 377-2004. Mais especificamente, esta norma está preocupada com o teste dos requisitos dos registros de troca de dados biométricos (*Biometric Data Interchange Records* (BDIR)) conforme definido no INCITS 423.1. Trata então dos ensaios de conformidade dos requisitos CBEFF, conforme estabelecido no INCITS 377-2004 que não está dentro do escopo da norma citada. Além disso, esta norma não está preocupada com os testes de outras características dos produtos biométricos (tal como requisitos não-funcionais) ou outros tipos de testes de produtos biométricos (ou seja, a aceitação, o desempenho, a robustez e a segurança). Qualquer organização que contempla o uso de métodos de ensaio definidos nesta parte da norma geral, deve considerar cuidadosamente as restrições sobre a sua aplicabilidade. Trada dos dois tipos (A e B) e três níveis (1, 2 e 3) de testes de conformidade que estão definidos no INCITS 423.1. No entanto, apenas o tipo A e os Níveis 1 e 2 estão dentro do escopo desta parte.
- ANSI INCITS 423.4-2009 - *Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 4* (*Conformance Testing Methodology for* INCITS 381- 2004, *Finger Image-Based*): esta parte do ANSI INCITS 423 está preocupada com os ensaios de conformidade das implementações buscando conformidade com o padrão de troca de mensagens das imagens de digitais (*Finger Image-Based Data Interchange Format*) definido na ANSI INCITS 381-2004. Além disso, esta parte da norma INCITS 423 está preocupada com os testes apenas dos requisitos do registro de troca de mensagens de dados biométricos (*Biometric Data Interchange Records* - BDIR), conforme definido na norma ANSI INCITS 381-2004. Esta parte do ANSI INCITS 423 não está preocupada com os testes de outras características dos produtos

biométricos ou outros tipos de testes de produtos biométricos (ou seja, a aceitação, o desempenho, a robustez e a segurança). Qualquer organização que contemple o uso de métodos de ensaio definidos nesta parte do ANSI INCITS 423 deve considerar cuidadosamente as restrições sobre a sua aplicabilidade. Para os casos de teste e assertivas que definem métodos e procedimentos de teste de nível 3 e Tipo B estão incluídas, nesta parte do ANSI INCITS 423, materiais apenas como informativos.

3.4.5 Padrões de Perfis de Uso Específico para Processos Biométricos

- ANSI INCITS 383-2004 - *Information Technology, Biometric Profile and Interoperability and Data Interchange/Biometrics-Based Verification and Identification of Transportation Workers*: especifica o perfil de aplicação de apoio a identificação e verificação de funcionário do setor de transportes do EUA, através da utilização de dados biométricos recolhidos durante a inscrição, nos pontos de acesso locais (ou seja, portas ou outras entradas controladas) e além das fronteiras locais, dentro de áreas definidas de controle. Ela define um conjunto de bases normativas e critérios para aplicação desses parâmetros em aplicações nas quais os *tokens* são usados para controle de acesso e identificação de funcionários.
- ANSI INCITS 394-2004 - *Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management*: especifica um perfil biométrico para aplicações de gestão de fronteiras nos EUA. Ela define um conjunto de normas e critérios básicos para a aplicação em aplicativos que usam a biometria para autenticar a identidade dos não cidadãos que entram, ficam e/ou deixam os Estados Unidos.
- ANSI INCITS 421-2006 - *Biometric Profile – Interoperability and Data Interchange – DoD Implementations*: esta norma seleciona subconjuntos de padrões existentes que são utilizados na implementação de sistemas de dados biométricos. Entre as normas de referência presentes neste documento estão a definição de interfaces do BioAPI, do uso do ANSI / NIST ITL 1-2000, e EFTS do FBI (EUA). Ela descreve as configurações biométricas para uso em aplicativos militares, que processam e armazenam dados biométricos sobre as bases de prisioneiros de guerra do inimigo (*Enemy Prisoners of War* - EPW), de pessoas detidas, internadas e pessoas de interesse no que diz respeito à segurança nacional nos EUA.

- ANSI INCITS 422-2007 - *Application Profile for Commercial Biometric Physical Access Control*: especifica um perfil biométrico para aplicações de controle de acesso. Ela define um conjunto de normas e critérios básicos para a aplicação dessas normas em aplicativos que usam a biometria para autenticar a identidade de usuários solicitando acesso a uma instalação. Estabelece requisitos mínimos de conformidade para as partes biométricas de tais sistemas. Não pressupõem a utilização de qualquer tecnologia biométrica especial, nenhum meio de armazenamento de dados, de sistema operacional ou de cartão de mídia/ documentos.

3.4.6 Padrões Metodológicos de Conformidade para teste dos Padrões de Perfis de Uso Específico para Processos Biométricos

- ANSI INCITS 409.1-2005 - *Biometric Performance Testing and Reporting Part 1 - Principles*: primeira parte de uma norma multiparte que especifica um conjunto comum de metodologias e procedimentos a serem seguidos para a realização de testes de desempenho técnico e avaliações. Incluem-se as orientações que abordam questões relativas aos tamanhos necessários de ensaios, de estatísticas de desempenho, do relatório de erros, e de apresentação de resultados de desempenho. Este padrão se apresenta na forma de um *framework* que pode ser incorporado em uma abordagem *"end-to-end"* de testes do sistema ou a partir de uma perspectiva componente individual (testes de caixa-branca e de caixa-preta).
- ANSI INCITS 409.2-2005 - *Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology*: segunda parte da norma multiparte que especifica os procedimentos para a realização de testes on-line do desempenho de tecnologias biométricas.
- ANSI INCITS 409.3-2005 - *Biometric Performance Testing and Reporting Part* 3 - *Scenario Testing Methodologies*: terceira parte da norma multiparte que especifica os requisitos para testes e relatórios biométricos baseados em cenários (*cases* de testes).
- ANSI INCITS 409.4-2006 - *Biometric Performance Testing and Reporting – Part 4*: *Operational Testing Methodologies*: quarta parte da norma multiparte que especifica os requisitos para testes biométricos baseados em relatórios e testes biométricos. Ela fornece os requisitos para planejamento de teste, execução de testes e relatórios de ensaio que devem ser seguidas durante os testes

operacionais de sistemas biométricos.

- INCITS TR-45-2009 - *Biometric Performance Testing and Reporting - Part 7: Framework for Testing Methodologies for Specific Modalities*: este relatório técnico documenta os fatores de influência que podem afetar o desempenho de sistema de biométrico. Neste documento, os fatores são categorizados como ambiental, biológico, comportamental, de usabilidade, social e orientados para o projeto. Este relatório técnico apresenta a influência de cada fator por categorias, discute as categorias de fatores que pode influenciar o desempenho de cada modalidade e lista os protocolos de teste usados.

3.5 Outros padrões ISO para Processos Biométricos usando XML

- ISO/IEC 24709 – *BioAPI Conformance*: padrões de testes/conformidade para os pacotes XML de dados.
- ISO/IEC 29120 – algoritmos para teste de dados automatizados: Parte 1 - formato do relatório de testes e Parte 2 - dados de entrada para os testes
- Documento "SC37 XML *namespaces*, *data elements*, *schemas*, *and related items*": Define regras e elementos comuns.

4 ARQUITETURA DE REFERÊNCIA

4.1 Tópicos da Arquitetura de Referência

Nesta introdução são apresentados os elementos propostos para compor as informações pertinentes (tópicos) que serão tratados junto à arquitetura de serviços, principalmente do Contrato de Serviços (*WSDL*) e do esquema de mensagens utilizados (*XML Schemas*), que serão sugeridos e documentados a partir dos candidatos a serviços e das capacidades de serviços, segundo apontado nos perfis de serviços e de capacidades. A Figura 4.1 ilustra esses elementos e suas relações a seguir.

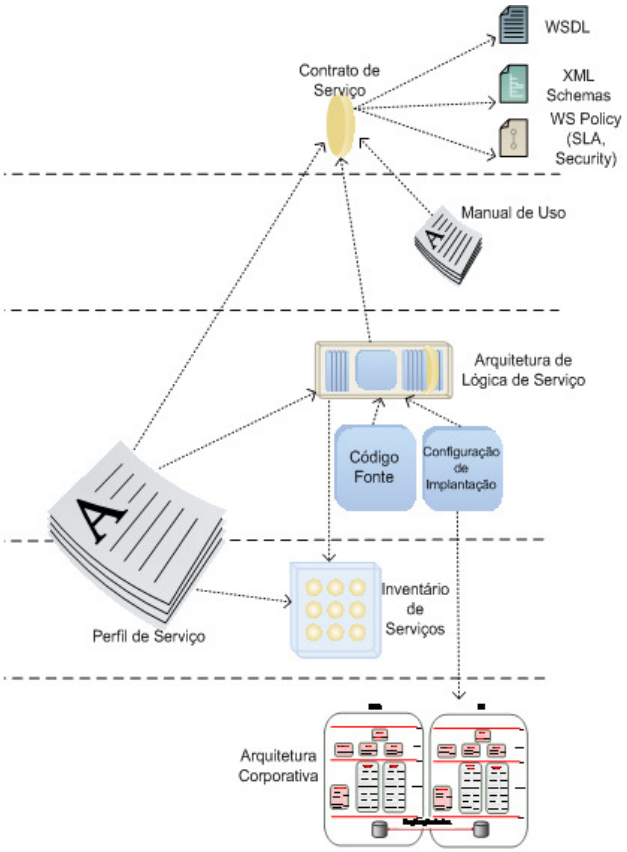


Figura 4.1. Níveis Arquiteturais e Modelos de Referência

*Nota: as definições de políticas de acesso e de SLA (*contidas nas definições de *WS-Policy) serão objeto de documentos posteriores, envolvendo os necessários requisitos de segurança e padrões mínimos de atendimento.*

4.2 Elementos da Arquitetura de Serviços (Servidor)

Para entendimento dos elementos da Arquitetura, lembramos que detalhes do elemento ESB na Arquitetura Corporativa ESB se encontram no relatório de ESB.

Ainda, detalhes do ABIS e do tratamento de armazenamento (camada de dados) são tratados em outros relatórios específicos. Os demais elementos da arquitetura serão examinados na seção a seguir.

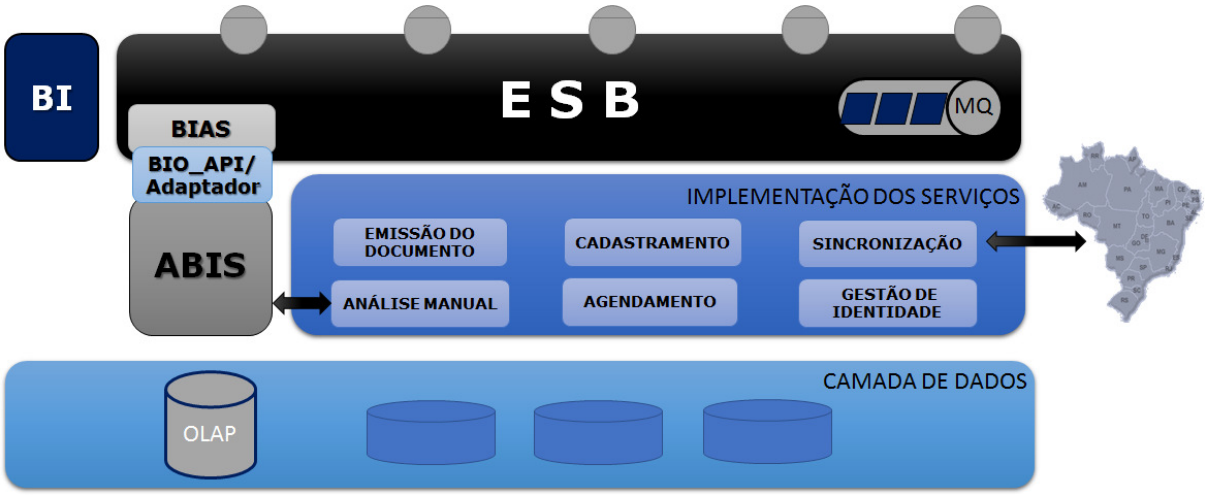


Figura 4.2. Arquitetura de Referência Proposta

4.2.1 *Business Intelligence* (BI)

Este elemento refere-se ao acesso à visão analítica do RIC, no que se refere a aplicação dos princípios de Inteligência de Negócios (BI) sobre os dados do RIC, visando dar suporte a geração de saídas gerenciais com o apoio de funções de ETL (extração, transformação e carga) do registros do RIC e dados populacionais; com saídas prevista que suportem análises demográficas, de perfis populacionais, etc. Cabe citar que, na solução proposta, existem dois conjuntos de soluções de BI a serem implementadas, a saber.

- Na disseminação de informações gerenciais para uso do Governo Federal durante todo o ciclo de vida de operação do RIC.
- No suporte gerencial a implantação do RIC, tal como na geração de percentuais de realização (pessoas cadastradas x população local) para análise e ajuste do esforço necessário para implantação do RIC.

4.2.2 Barramento Corporativo de Serviços (ESB)

Como elemento essencial ao estabelecimento do modelo sistêmico para o RIC, principalmente no que se refere a sua performance, a escolha de um ESB é um fator vital - em conjunto a soluções sistêmicas de armazenamento/recuperação de dados de alta performance - para atingimento dos objetivos do projeto em análise. Cabe citar que os requisitos e a melhor compreensão das funcionalidades de ESB´s são detalhadas em riqueza junto ao RT Estudo sobre Soluções de *Message Queue* / Barramento de Serviços Corporativos.

Cabe citar neste documento que, com o uso de soluções de ESB, requisitos sistêmicos comuns, tais como de *log* para auditoria, de segurança da informação (em parte), e de gerenciamento de requisitos de escalabilidade, já são realizados de maneira configurável (sem a necessidade de nenhuma atividade de desenvolvimento suplementar) pelos Barramentos Corporativos de Serviços (ESB's) profissionais.

4.2.3 BIAS

Da seção 3.1 deste documento, reportamo-nos ao que foi desenvolvido segundo a especificação "INCITS 442-2010 - Information Technology - Biometric Identity Assurance Services (BIAS)". Essa especificação apresenta um contexto mínimo de mensageria para o estabelecimento de um modelo de Biometria como Serviços ("Biometrics as a Service"), no que se refere as atividades de Cadastramento (Enrollment), Limpeza da Base (Screening), Autenticação (Authetication) e Geração de Credenciais (Credential).

Neste sentido, a troca de dados padrões entre os componentes que são os elementos que compõem essa arquitetura, busca atender os requisitos que estão contidos nas ISO da série 19794-1 - que estão especificadas em documentos diversos - conforme apontada na Figura 4.3.

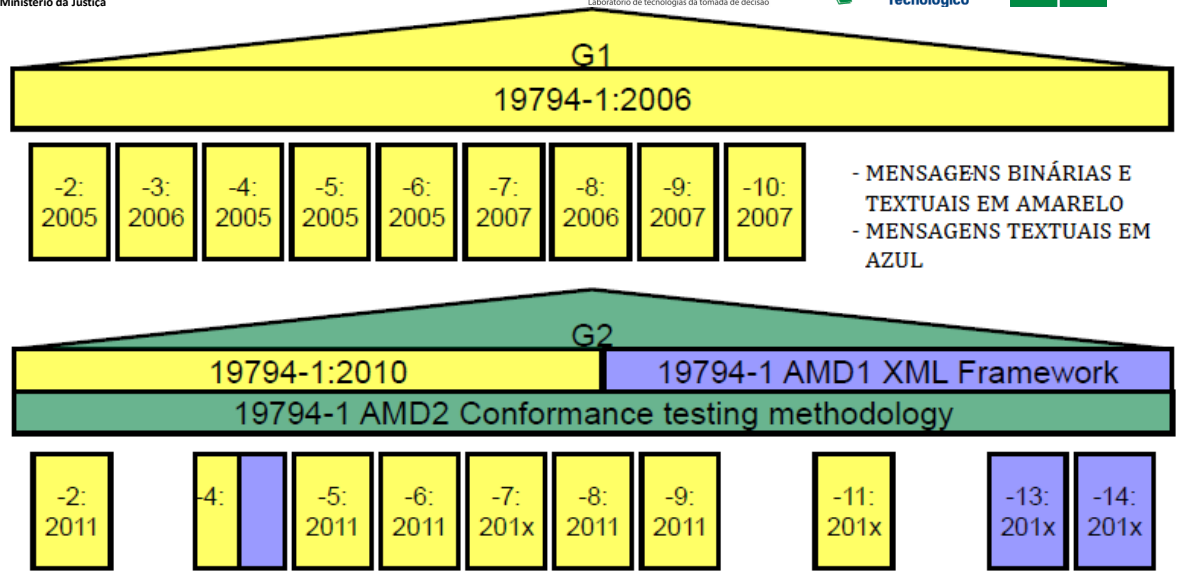


Figura 4.3. Divisões da ISO 19.794-1

Pela Figura 4.3, foi estudado que a ISO 19.794 tem na sua divisão G1, a especificação de um framework de mensagens para os seguintes aspectos.

- Minúcias de digitais (Finger minutiae)
- Séries temporais de Assinatura (Signature/sign time series)
- "Espectro" de padrões de digitais (Finger pattern spectral)
- Estrutura dos padrões de digitais (Finger pattern skeletal)
- Imagens de Digitais (Finger image)
- Imagens Vasculares (Vascular)
- Face (Face)
- Geometria da Mão (Hand geometry)

Ainda, na sua divisão G2, entende-se da especificação, um framework de mensagens para os seguintes itens.

- Imagens de digitais (finger image)
- Voz (voice)
- DNA
- Outros "por vir" (uso futuro)

Em resumo, essa especificação deu origem ao referencial "Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0", ora já citado neste documento, que especifica como utilizar os arquivos XML definido na norma ANSI INCITIS 442-2010 (baseado na troca de mensagens da ISO 19.794) para invocar serviços baseados em SOAP para sistemas de registro e de identificação biométrica, habilitando a utilização remota de serviços de identificação biométrica em uma estrutura SOA que atenda as capacidades de serviços como ilustrado Figura 4.3.

Figura 4.3 - Capacidades / Funcionalidades Básicas

Nota: Existe uma implementação de referência oferecidos pela NIST - uma implementação em Visual Basic sem interesses comerciais - para exemplificar como elaborar uma arquitetura de serviços biométrica básica para um sistema similar ao RIC, no link: <http://www.nist.gov/itl/iad/ig/upload/BIAS_20130114.zip>

Dada as normas e suas especificações, os serviços oferecidos pela interface BIAS:

- são compostos de operações modulares e independentes, que podem ser montadas de diversas formas diferentes para apoiar uma variedade de processos de negócios de registro/verificação biométrica (capacidades ligados em composições formando serviços de tarefa complexos);
- podem ser implementadas usando diferentes tecnologias em múltiplas/ diversas plataformas;
- podem ser expostos (publicados) de forma direta e /ou indireta através de um prestador de serviços ao modelo proposto pela SOA.

4.2.4 BIO API

O documento ISO/IEC - 19784-1 - *Biometric Application Programming Interface - Part 1 - BioAPI Specification* especifica uma estrutura que provê um modelo arquitetural que permite que componentes de um sistema biométrico sejam providos por diferentes fornecedores e ainda assim sejam completamente interoperáveis através de API's, (que para atender devem estar padronizadas segundo a ISO já citada) segundo ilustrado na Figura 4.4.

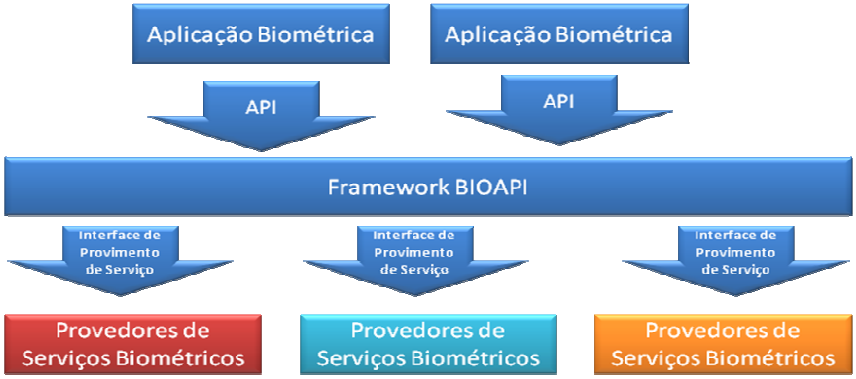


Figura 4.4 - Funcionamento da BIOAPI

Nesse sentido, assim como o fornecimento de serviços BIOS API segue um padrão, a BIOS API (utilizada pelos serviços BIAS) também segue, estabelecido na ISO/IEC - 19784-1. Todas essas especificações seguem um modelo de troca de mensagens no formato ilustrado na Figura 4.5.

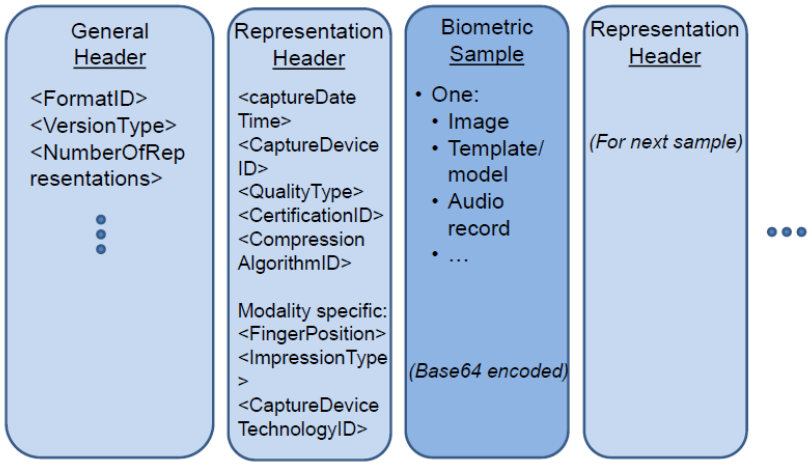


Figura 4.5 - Mensagens da interface BIAS e da interface BioAPI

A especificação BioAPI é um padrão aberto de interface de programação de aplicações (API) que permite que aplicativos de *software* para se comunicar com uma ampla gama de tecnologias biométricas de uma forma comum. Assim, no que se refere à comunicação, o uso desse padrão pode ser usado tanto no cliente quanto em um modelo de centralização de dados através de *webservices*, tal como ilustrado na Figura 4.6 na marca [3].

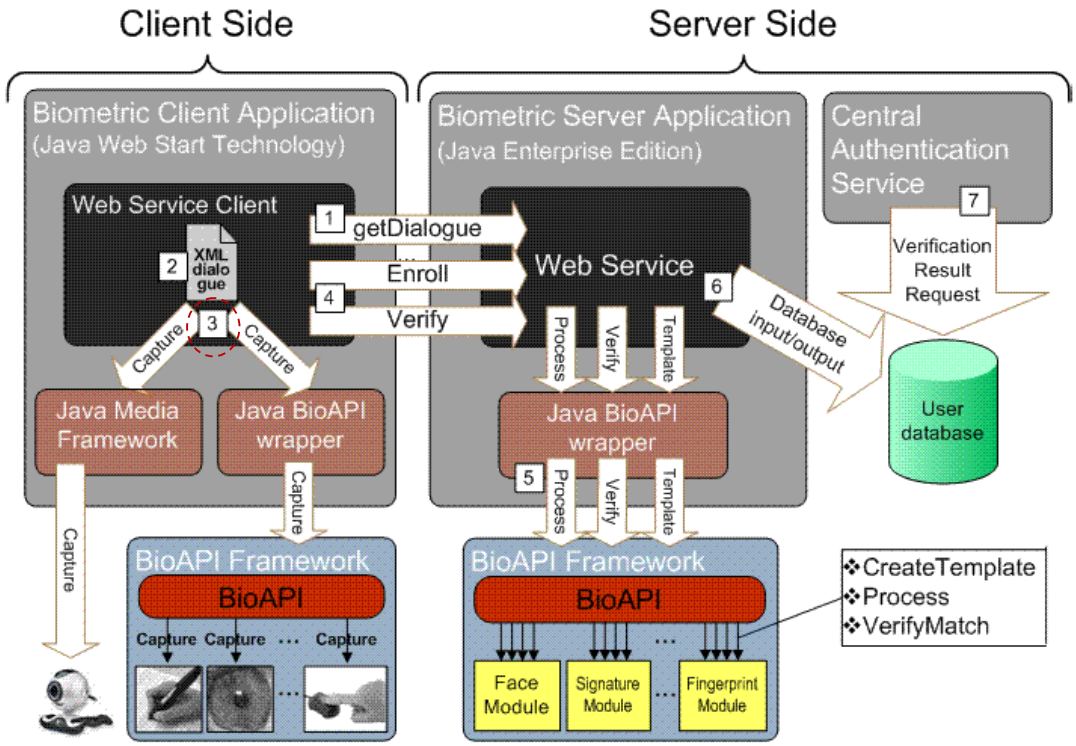


Figura 4.6 – Uso da BioAPI tanto no lado da aplicação cliente quanto da servidora

Nota: da Figura 4.6, temos no Web Service Client tanto o processo simples de captura para encaminhamento e com equipamentos sem conformidade com a BioAPI usando qualquer Java Media Framework, ***OU*** *o uso de todo o processo de captura através da BioAPI (dois fluxos saindo de Web Service Client saindo da marca em [3] em destaque).*

Para dar entendimento ao padrão, cabe apontar sua evolução a partir de versões de interface até sua declaração como padrão ANSI e ISO/IEC (Figura 4.7).

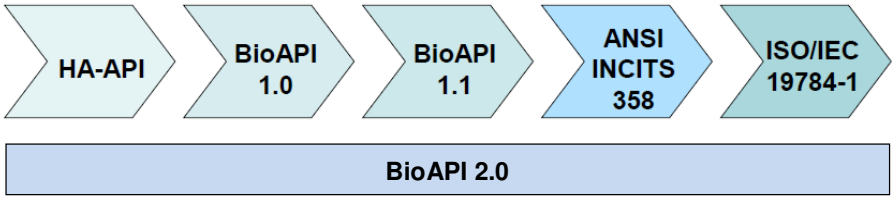


Figura 4.7 – Evolução do padrão BioAPI

Ainda, a ISO/IEC 29141:2009 especifica os requisitos para a utilização da ISO/IEC 19784-1 com a finalidade de realizar uma operação de captura *Tenprint*. Essa ISO especifica um formato de bloco de dados biométricos que é utilizado para interagir com uma estrutura BioAPI, e, portanto, com define como prestadores de serviços biométricos (BSP) podem suportar uma aplicação que pretenda realizar uma captura *Tenprint*.

São grupos de funções (requisitos a serem tratados) da BioAPI, a saber.

- Operações Biométricas
- Operações de Armazenamento e Recuperação (DB)
- Operações Primitivas (Unitárias)
- Funções de Gerenciamento dos Componentes
- Operações de Manipulação de dados
- Operações de *Callback* e de Eventos
- Funções Utilitárias

Desses Grupos temos as funções básicas e as primitivas, a saber.

a) Funções Básicas

- Cadastro (*Enroll*): cria um *template* (armazenado em conta de usuário do banco de dados e/ou BSP DB).
- Verificação de Identidade 1:1 (*Verify*): entrada e comparação contra um elemento.
- Descoberta de identidade 1:N (*Identify*): entrada e comparação contra todos

os *templates* gravados.

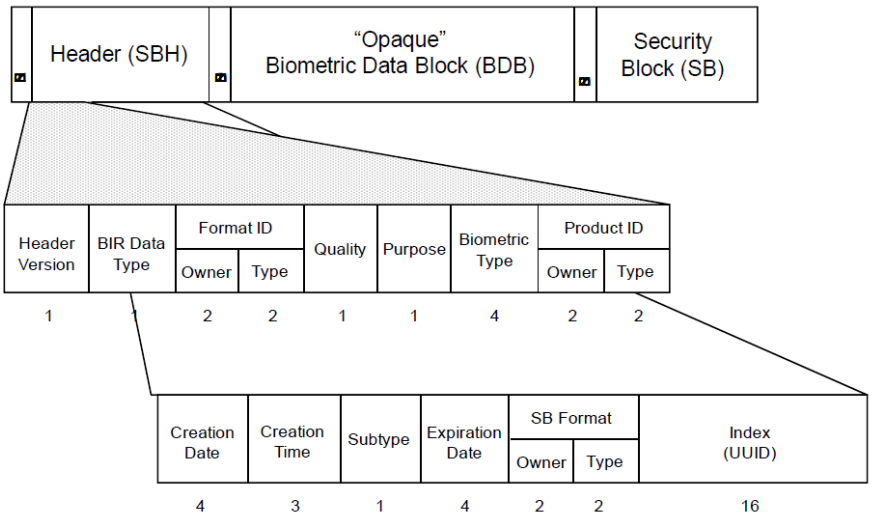
b) Funções Primitivas

- Captura (*Capture*): captura de dados biométricos a partir do sensor.
- Criação de *Template* (*CreateTemplate*): cria um *template* para um dado bruto, sendo que o novo *template* pode ser uma adaptação de um *template* armazenado
- Processamento (*Process*): converte o dado intermediário para um dado de BIR processado para correspondência.
- Processamento com BIR Auxiliar (*Process with Aux BIR*).
- Comparação (*VerifyMatch*): realiza a comparação 1:1.
- Identificação (*IdentifyMatch*): realiza a comparação 1:N contra um DB
- Importação (*Import*): importa dados em "*batch*" (não em tempo real) para o processamento.

Ainda, são recursos opcionais da BioAPI os descritos a seguir.

- Retorno dos dados brutos gravados ou de dados de auditoria.
- Retorno dos fatores de qualidade ora realizados.
- Chamadas de *"streamers"* de dados por GUI.
- Possibilidade de aplicações de técnicas de pré-processamento de dados (*binning*).
- Assinatura na recepção/gravação de BIR's.
- Criptografia de BIR's.
- Retorno do FRR.
- Modelo adaptativo de *templates* e outros.
- Flexibilidade na configuração das operações básicas e das operações primitivas.

O pacote utilizado (BIR) tem a seguinte estrutura.




```
<?xml version='1.0' encoding="utf-8"?>
    <xs:schema
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns=" urn:oid:1.1.19785.0.257.1.7.0"
        targetNamespace=" urn:oid:1.1.19785.0.257.1.7.0"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">

        <xs:element name="bir" type="BIR"/>

        <xs:complexType name="BIR">
            <xs:sequence>
                <xs:element name="version" type="Version" minOccurs="0"/>
                <xs:element name="cbeff-version" type="Version" minOccurs="0"/>
                <xs:any namespace="##other" processContents="skip"
                        minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="bir-info" type="BIR-info"/>
                <xs:element name="bdb-info" type="BDB-info" minOccurs="0"/>
                <xs:element name="sb-info" type="SB-info" minOccurs="0"/>
                <xs:element name="bir" type="BIR"
                        minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="bdb" type="xs:base64Binary" minOccurs="0"/>
                <xs:element name="sb" type="xs:base64Binary" minOccurs="0"/>
            </xs:sequence>
        </xs:complexType>
```

Figura 4.8 – Estrutura/Payload do Pacote Básico do BioAPI

Nota: o bloco (SB) é opcional

Para uso em Provas de Conceito, na falta de uma implementação suficiente, lembramos que a NIST escreveu um pacote de domínio público - NIST *Biometric Software Imagem* (NBIS) - que inclui o algoritmo de correspondência de impressão digital BOZORTH3. Ele é escrito em ANSI C para que ele irá compilar e rodar em Linux. Para usar BOZORTH3, primeiro você tem que executar suas impressões digitais através do detector de minúcias MINDTCT que também está incluído no NBIS. (NIST *Biometric Image Software* <http://www.nist.gov/itl/iad/ig/nbis.cfm>).

4.2.5 Implementação dos Serviços

As implementações SOA dependem de uma rede de serviços de *software*. Serviços incluem baixo acoplamento de unidades e de funcionalidade. Cada serviço implementa uma ação, como preencher um formulário *on-line* de uma aplicação ou visualizar um extrato bancário de uma conta, ou realizar uma reserva *on-line* para bilhete de avião. Ao invés de realizar de chamadas diretas para o código fonte, os serviços definem protocolos que descrevem como enviar e receber as mensagens. Geralmente, em estruturas de mensagens, são descritas em arquivos de esquema XML (XML Schema). Assim a troca de mensagens se dá por pacotes de dados em formato XML (Wikipedia).

Cada declaração de capacidade/operação de um serviço em seu Contrato (elemento "CONTRATO" na Figura 4.9) se assemelha à uma funcionalidade de uma API. Esses Contratos tem um "ponteiro" (*bind*) para lógicas compiladas (elemento "LÓGICA" na Figura 4.9). Agentes intermediários de pré-processamento e códigos de "fachada" entre a LÓGICA do serviço e a infraestrutura podem ser ainda implementados. Todos esses elementos desacoplam (desassociam) as chamadas oferecidas aos sistemas externos da lógica (programa) que as executa.

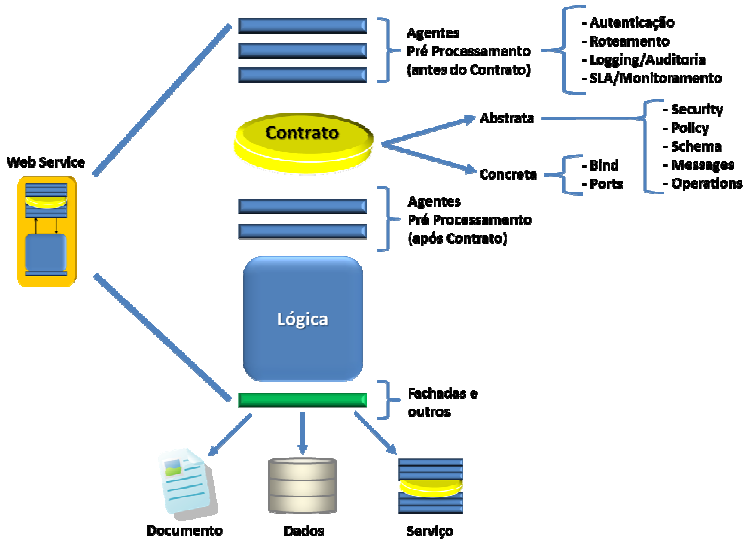


Figura 4.9 – Elementos da estrutura de um serviço SOA

4.2.6 Camada de Dados

Por fim, a arquitetura proposta prevê a existência de elementos distintos no que se refere a camada de armazenamento de dados. O modelo proposto prevê uma Hierarquia de bancos de bancos por perfil dos dados [16]

Quanto ao uso de ferramentas, soluções sistêmicas e SGBDs tradicionais, este documento não propõe obrigatoriamente o uso de MySQL como SGBD, de HBase como solução de armazenamento de dados de alta performance e de NFS como solução de armazenamento de dados em disco, mas apenas dá nome aos tipos de armazenamentos que podem ser utilizados. Outras soluções de armazenamento similares podem ser utilizadas, mas essas são as soluções propostas na construção da prova de conceito a ser realizada em decorrência deste.

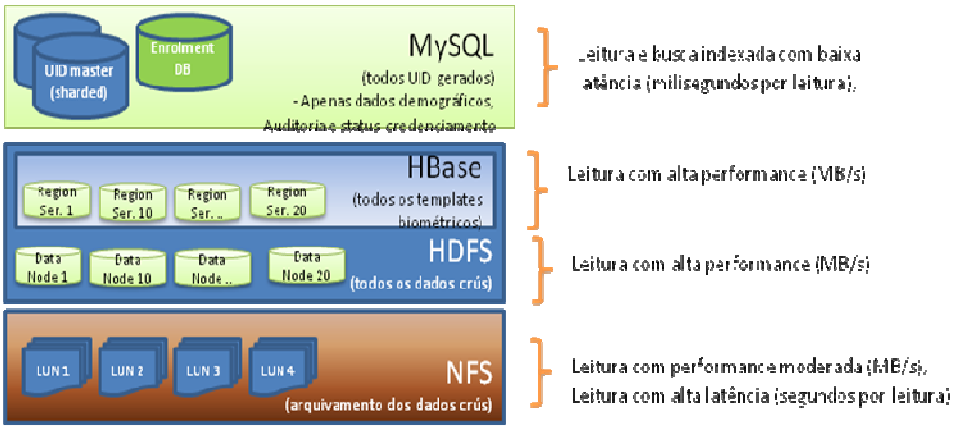


Figura 4.10 – Elementos da estrutura de um serviço SOA

Assim, entenda-se da Figura 4.10 o termo MySQL como a pré-existência de um modelo de SGBD relacional; de HBase, a existência de um modelo de baixa latência para consulta (verificação e identificação); e de NFS, como um modelo de alta performance no armazenamento de dados binários, tal como as imagens digitais das biometrias (dedos, fotos, etc.).

Sobre as questões de armazenamento seguro de dados biométricos, os mesmos são definidos através da ISO/IEC 24745:2011 - *Information technology -- Security techniques - Biometric information protection*. Esta ISO provê um guia para proteção da informação biométrica em relação aos requisitos de confidencialidade, integridade, renovabilidade/ revogabilidade durante o armazenamento e transferência; além de fornecer requisitos e

orientações para a gestão e tratamento seguro e com respeito à privacidade de informações biométricas.

4.2.7 Transmissão e Interoperabilidade de Dados

Ainda para garantia de segurança nos dados, dado o modelo prever uma arquitetura cliente/servidor, processos de criptografia são projetados em toda extensão da relação cliente servidor. O cliente criptografa dados que são encaminhados ao servidor que irá descriptografar e tratara consistência e validade dos dados garantidos, dada sua origem. A Figura 4.11 ilustra esse modelo de garantia de segurança no canal de transmissão. Maiores detalhes dessa implementação são apontados junto ao *RT Diretrizes em Segurança da Informação*.

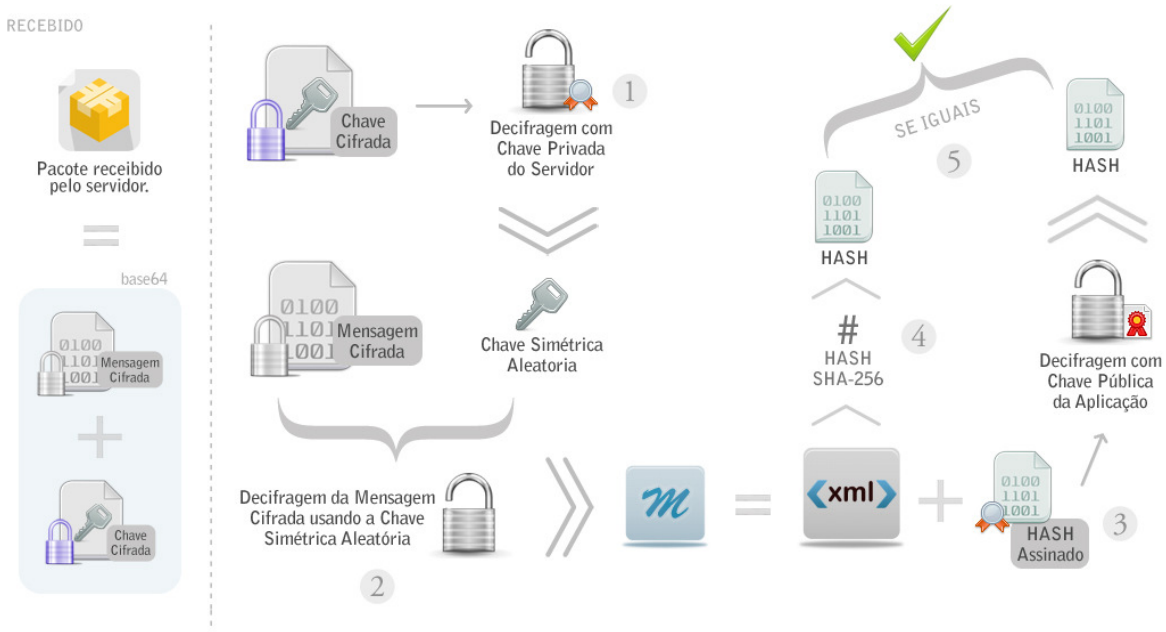


Figura 4.11 – Elementos da estrutura de um serviço SOA

Dos padrões de interoperabilidade de dados a serem utilizados, é importante o (re-) conhecimento do uso dos seguintes padrões (que devem ser estudados e utilizados por Arquitetos e Desenvolvedores da solução baseada em SOA com o suporte de um *middleware* orientado a mensagens).

- ISO.IEC - 19794-2 - IT - *Biometric Data Interchange Formats - Part 2 - Finger Minutiae Data*
- ISO.IEC - 19794-4 - IT - *Biometric Data Interchange Formats - Part 4 - Finger Image Data*
- ISO.IEC - 19794-6 - IT - *Biometric Data Interchange Formats - Part 6 - Iris Image Data*
- ISO.IEC - 19794-5 - IT - *Biometric Data Interchange Formats - Part 5 - Face image data*
- ISO/IEC 19794-7:2014 - IT- *Biometric data interchange formats - Part 7: Signature/sign time series data*

4.3 Arquitetura Sugerida para as Soluções Clientes

4.3.1 Especificação para os Dispositivos Biométricos *(WS-Biometric Devices)*

Nesta seção, reportamo-nos ao padrão "NIST *Special Publication* 500-288 v1 - *Specification for WS-Biometric Devices* (WS-BD) v1" que provê um *framework* para implementar e invocar as operações básicas para comandar e controlar sensores biométricos através da utilização de protocolos leves de serviços web (*"lightweight web service protocols"*) de forma a maximizar a interoperabilidade destes dispositivos. Neste sentido, existem duas formas de atuar como clientes de um sistema biométrico.

A Figura 4.12 ilustra (em (a) e (b)) esses modelos.

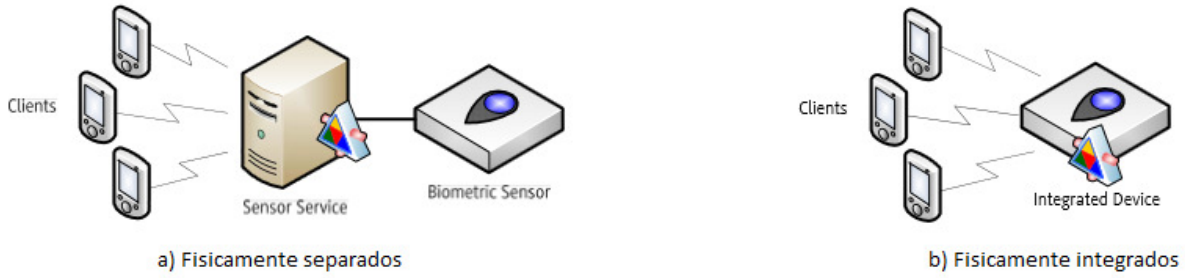


Figura 4.11 – Modelos de implementações de Clientes para Processos Biométricos

Do uso de padrões inteoperáveis, pode-se destacar o uso do padrão NIST SP 500-288, o qual especifica um serviço Web baseado em TCP/IP e HTTP(S) para comando e controle de dispositivos de aquisição de biométricos que tem como metas: permitir a interoperabilidade biométrica multimodal; melhorar a identificação móvel e autenticação remota; estabelecer uma comunicação multi-plataforma e independente do dispositivo. Com a definição desse padrão (WS-BD), temos então no modelo global uma arquitetura de protocolos interoperáveis como ilustrado na Figura 4.12.

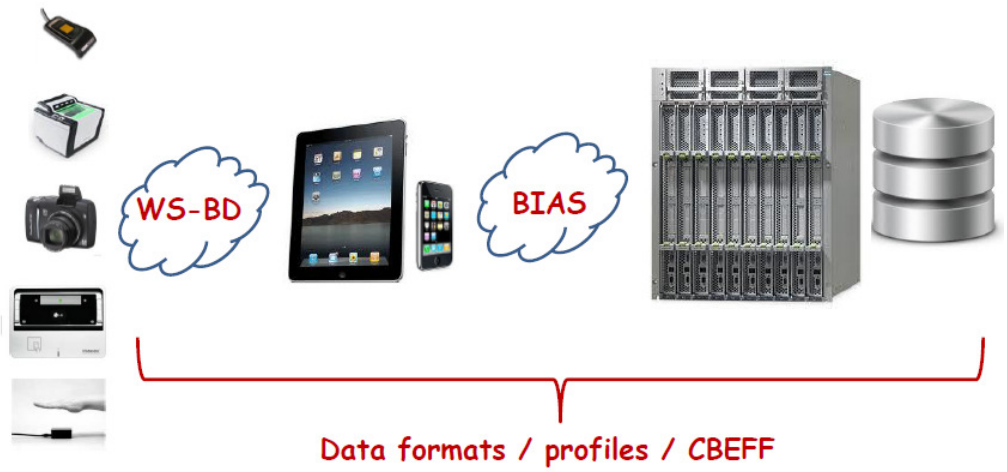


Figura 4.12 – Formatos e Implementações Interoperáveis na relação cliente/servidor

5 SERVIÇOS E CAPACIDADES

5.1 Introdução

Na continuidade da análise contida neste documento, é importante que se ignore sua estrutura, e que se avance em seu conteúdo para o que se descreve no Anexo C do documento, isto é, para os diagramas de sequência ilustrados (erroneamente definidos como *Use Cases* na documentação original).

Na descrição deste anexo, temos sua intenção declarada de “fornecer gráficos diagramas de sequência/fluxo-operacional que mostram como os cenários mais elevados dos níveis de utilização no contexto do [INCITS-BIAS] poderia ser implementado utilizando o perfil BIAS SOAP”.

Trazendo clareza a essa declaração, esses diagramas ilustram o contexto de atividades/composição de serviços sugeridas de forma a atender os macroprocessos essenciais de um projeto de registro biométrico: dos métodos mais básicos (primitivas) de Verificação, de Identificação e de Inscrição; e das capacidades operacionais de verificação síncrona unitária e/ou em lote, verificação assíncrona unitária e/ou em lote, e de inscrição em lote.

Essas representações dão entendimento às composições de serviços (um serviço é aquilo que dispara um processo sequencial de chamada de serviços mais “primitivos”) necessárias para o funcionamento das tarefas complexas do provimento de serviços do BIAS.

Junto ao diagrama correspondente, a seguir é detalhado o proposto como idealizado, assim como é apontado os padrões de mensagens em relação ao que já foi elencado no padrões e normas citados.

a) Serviço composto de Verificação (natureza de resposta síncrona).

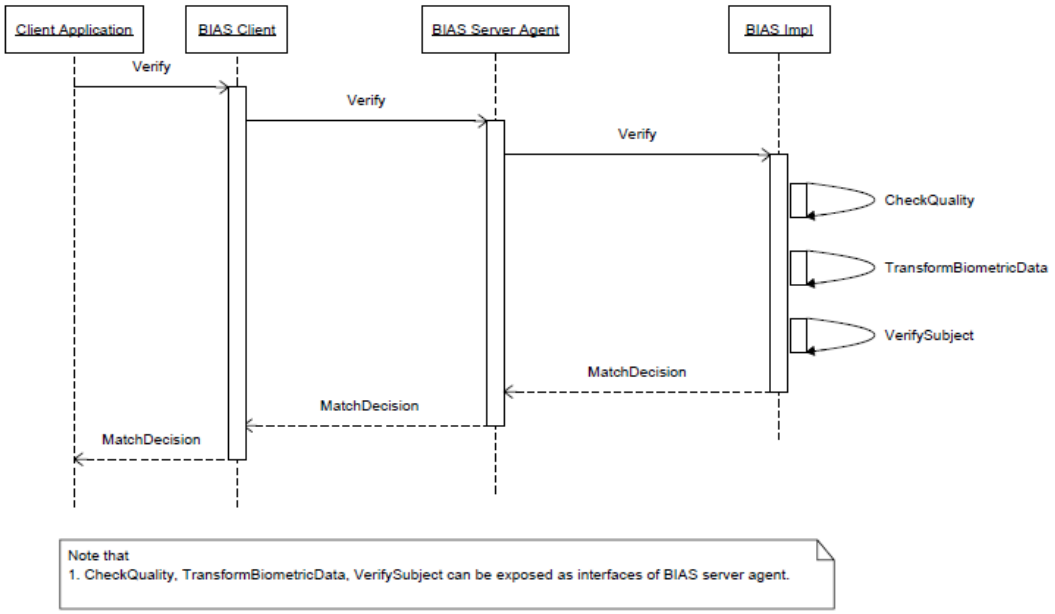


Figura 5.3 - Diagrama de Composição do Serviço Verificação (1:1) síncrono

A Figura 5.3 ilustra o diagrama que realiza o serviço composto de Verificação (***Verify***), em que uma única solicitação resulta em um conjunto de operações (neste caso, uma série de operações primitivas) que está sendo executada pelo servidor BIAS. A resposta ao serviço é diretamente o consumo da resposta ao serviço composto ***Verify***.

Cabe registrar, desde já, que a operação ***CheckQuality*** refere-se a uma atividade interna de teste de integridade em todo conteúdo/formato da mensagem repassada, sendo considerada como atividade inicial de qualquer realização de serviços de BIAS, assim, constando de todos os diagramas a seguir.

b) Serviço composto de Verificação (natureza de resposta assíncrona).

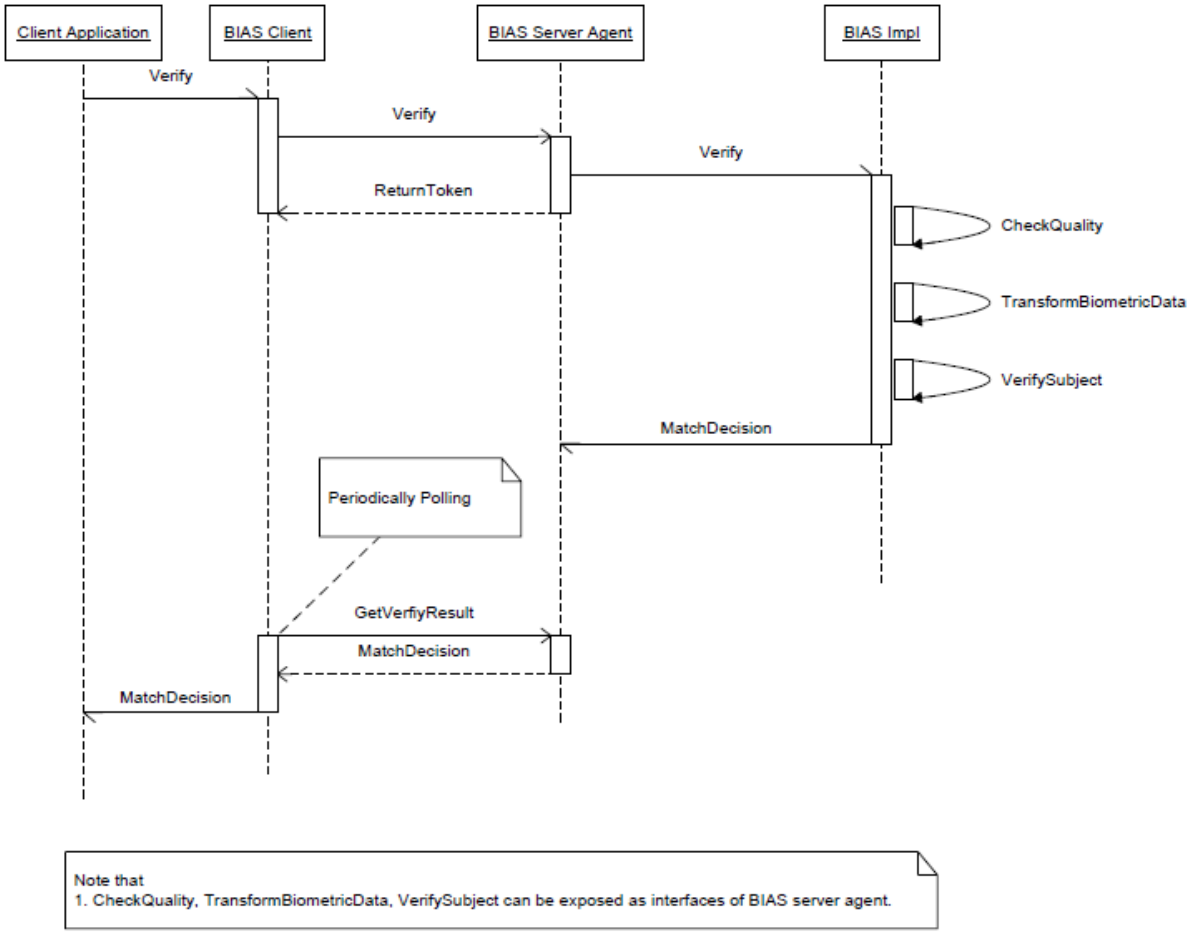


Figura 4.4 - Diagrama de Composição do Serviço Verificação (1:1) assíncrono

A Figura 5.4 ilustra o diagrama que realiza o serviço composto de Verificação em uma natureza assíncrona. Neste caso de uso, o solicitante emite duas requisições em momentos díspares: o pedido assíncrono de verificação (serviço primitivo BIAS ***Verify***), que retorna um *token* da operação solicitada (tal qual um número protocolo), seguido da operação ***GetVerifyResult*** para recuperar os resultados dessa operação.

Note-se que somos formalmente desfavoráveis ao uso de modelos de "pooling" (requisições sucessivas temporizadas ao servidor até que o mesmo tenha a resposta desejada. Novos protocolos, tais como o uso de modelo de mensageria *Publish-Subscribe* pode ser usado para esse fim.

c) Primitiva de Verificação (método mais básico usado em outros serviços).

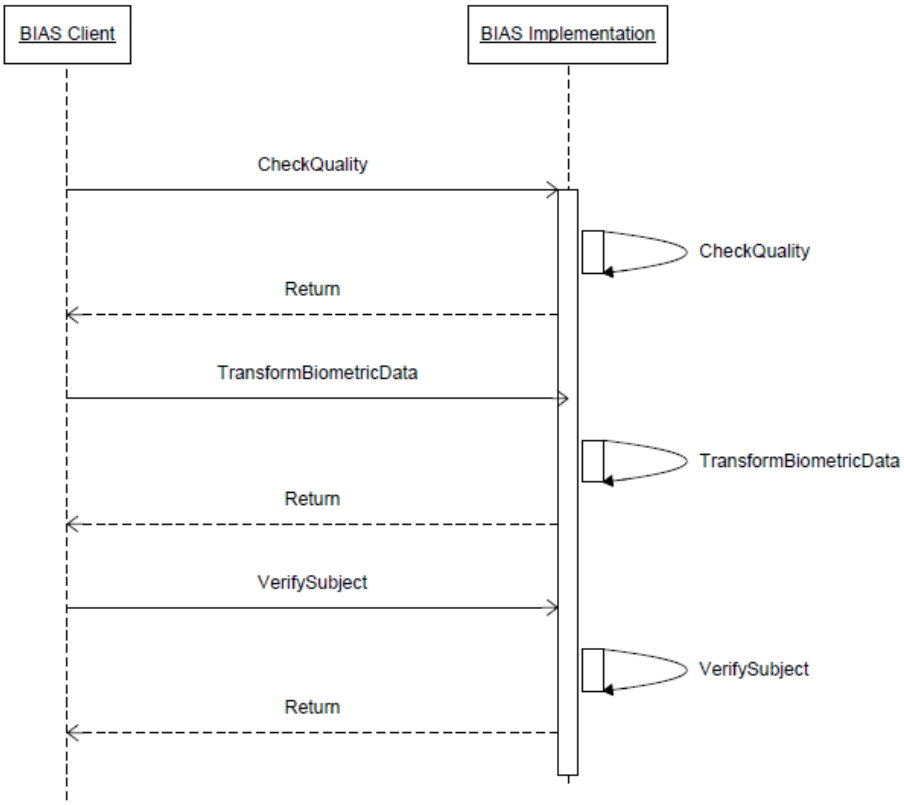


Figura 5.5 - Diagrama de Processo na Chamada Sequenciada para Verificação

Neste caso, o processo de verificação se dá por uma série sequenciada de requisições de primitivas BIAS (***CheckQuality***, ***TransformBiometricData***, ***VerifySubject***). Assim, cabe a aplicação cliente, o controle desse fluxo de requisições e os possíveis erros ocorridos (Figura .5.5).

d) Primitiva de Identificação (método mais básico)

A Figura 5.6 ilustra o uso do serviço composto de identificação (*Identity* - 1:N) em que uma única requisição executa a composição de uma série de operações (neste caso uma sequência de chamada para operações de primitivas BIAS (***CheckQuality,*** ***TransformBiometricData*** **e** ***IdentifySubject***) que são realizadas em conjunto no âmbito do servidor BIAS. O retorno se dá em uma lista de candidatos (*CandidateListType*) como elencado na relação de tipagens apontadas neste tópico deste documento.

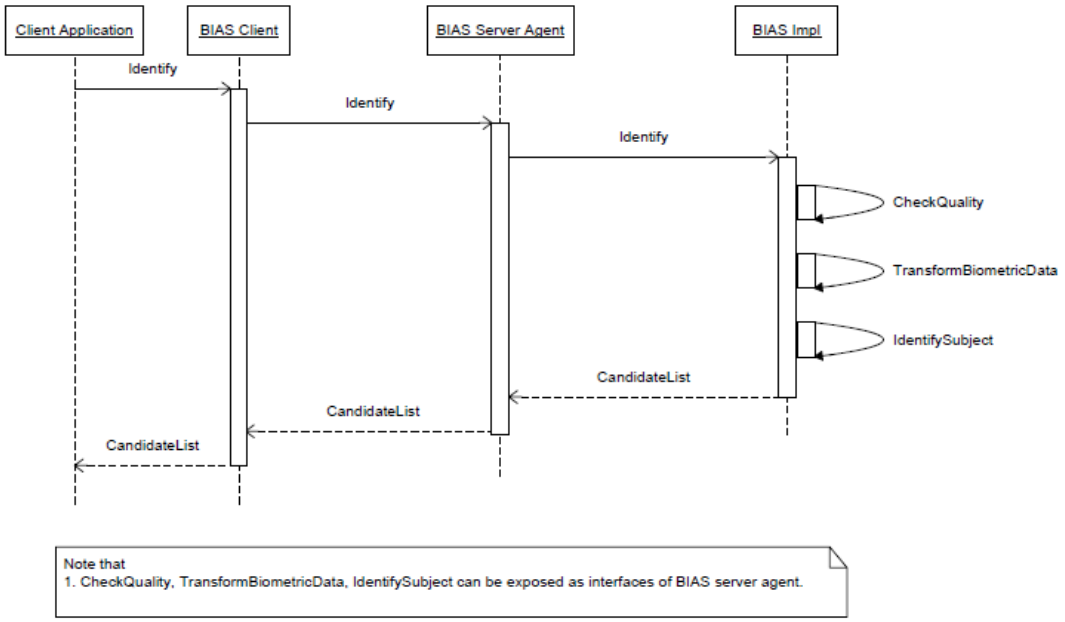


Figura 5.6 - Diagrama de Composição do Serviço Identificação (1:N) síncrono

e) Serviço de Tarefa Complexo de Cadastramento (composição de serviços).

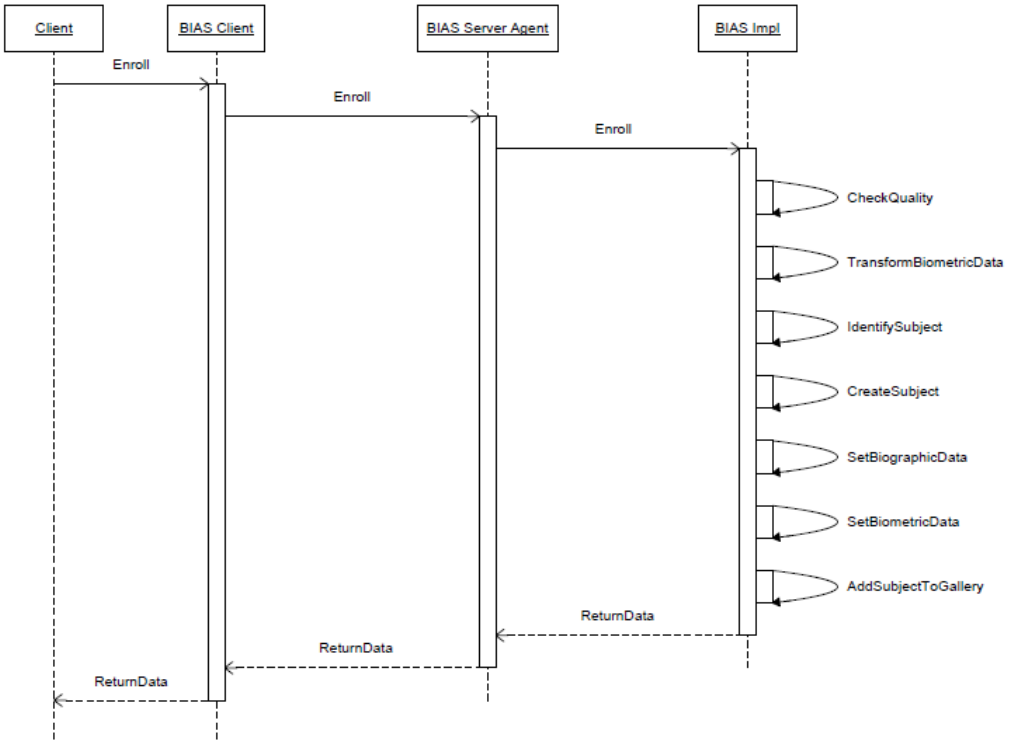


Figura 5.7 - Diagrama do Serviço Composto de Cadastramento ("*Enroll*")

A Figura 5.7 ilustra o uso do serviço composto de cadastramento (*Enroll*), em que

uma única requisição executa a composição de uma série de operações (neste caso uma sequência de chamada para operações de primitivas BIAS (***CheckQuality,*** ***IdentifySubject***, ***CreateSubject***, ***SetBiographicData***, ***SetBiometricData***, ***AddSubjectToGallery***) que são realizadas em conjunto no âmbito do servidor BIAS.

Assim, caso o resultado do processo *IdentifySubject* não retorne nenhum registro, o indivíduo é adicionado na galeria. Caso o resultado retorne algum registro, alguma outra ação pode ser executada (ex: retornar a lista de candidatos, adicionar "situação" para um indivíduo já existente, etc.).

f) Primitivas de Cadastramento (sequencia de processos).

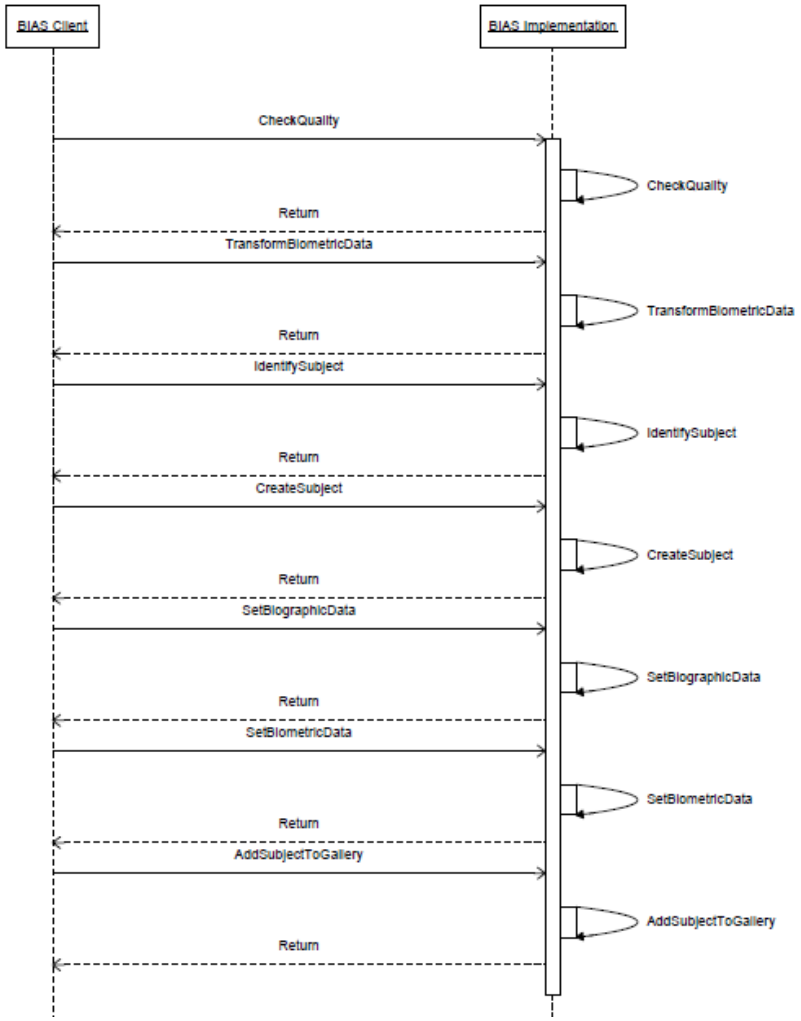


Figura 5.8 - Diagrama de Cadastramento como Sequencia de Chamadas

Nesse caso, o processo de cadastramento se dá por uma série sequenciada de requisições de primitivas BIAS (***CheckQuality***, ***TransformBiometricData***, ***VerifySubject,***

CreateSubject, SetBiographicData, SetBiometricData, AddSubjectToGallery).

Assim, cabe a aplicação cliente ao controle desse fluxo de requisições e os possíveis erros ocorridos (Figura 5.8).

5.2 Capacidades / Operações de Serviços Definidas

A seguir agrupamos as capacidades/operações de serviços definidas para serem executadas nos processos do BIAS.

a) Serviços de Cadastramento:

- Criar indivíduo (<wsdl:operation name="CreateSubject">): cria um novo registro de indivíduo, e associa um ID a esse registro.
- Apagar indivíduo (<wsdl:operation name="DeleteSubject">): exclui um registro de indivíduo existente e, em um modelo de centrado em situações ("*encounter-centric*"), apaga qualquer informação associada a situação de um indivíduo.
- Adicionar indivíduo na galeria (<wsdl:operation name="AddSubjectToGallery">): registra um sujeito a uma determinada população ou "situação".
- Excluir indivíduo na galeria (<wsdl:operation name="DeleteSubjectFromGallery">): remove o registro de um indivíduo em uma galeria ou "situação".

b) Serviços para gerenciamento de informações cadastradas (atualização e consulta).

- Definir Dados Biográficos (<wsdl:operation name="SetBiographicData">): associa dados biográficos com um determinado registro indivíduo; podem substituir os dados existentes ou criar um novo "situação"
- Atualizar/Excluir dados biográficos (<wsdl:operation name="UpdateBiographicData">, <wsdl:operation name="DeleteBiographicData">): atualiza / remove dados biográficos de um determinado indivíduo ou "situação".
- Listar Dados Biográficos (<wsdl:operation name="ListBiographicData">): lista os elementos de dados biográficos armazenadas de um indivíduo ou "situação".
- Obter informações biográficas (<wsdl:operation

name="RetrieveBiographicInformation">): recupera os dados biográficos associados à um indivíduo ou "situação".

- Definir os dados biométricos (<wsdl:operation name="SetBiometricData">): associa dados biométricos com um determinado registro indivíduo ou podem substituir os dados existentes ou criar um novo "situação".
- Atualizar / Excluir dados biométricos (<wsdl:operation name="UpdateBiometricData">, <wsdl:operation name="DeleteBiometricData">): atualiza/remove dados biométricos de um determinado indivíduo ou "situação".
- Listar dados biométricos (<wsdl:operation name="ListBiometricData">): lista os elementos de dados biométricos armazenados em um indivíduo ou "situação".
- Recuperar dados biométricos (<wsdl:operation name="RetrieveBiometricInformation">): recupera os dados biométricos associados a um indivíduo ou "situação".

c) Serviços Primitivos de Verificação/Identificação.

- Verificar indivíduo (<wsdl:operation name="VerifySubject">): executa uma verificação 1:1 entre um dado biométrico e um pedido de autenticação de um indivíduo em uma dada galeria.
- Identificar indivíduo (<wsdl:operation name="IdentifySubject">): executa uma pesquisa de identificação contra uma determinada galeria para um dado biométrico, retornando uma lista de candidatos ordenados segundo um *rank* de um tamanho máximo determinado.
- Verificar qualidade de dados passados (<wsdl:operation name="CheckQuality">): retorna um índice de qualidade para um determinada entrada de dados biométrico.
- Classificar dados biométricos (<wsdl:operation name="ClassifyBiometricData">): realiza o processo de classificação de uma entrada de dados biométrica.
- Realizar a fusão (<wsdl:operation name="PerformFusion">): aceita tanto *match* por escore ou por informações para tomada de decisão e cria um resultado de fusão pelo *match* associado.

- Transformar dados biométricos (<wsdl: nome da operação = "TransformBiometricData">): transforma ou processa um dado em formato biométrico em outro formato (por exemplo, extrações, centralização e de culturas, Conversão de formato de Dados).

d) Serviços Compostos /de Processamento / de Tarefas Complexas.

- Cadastrar (<wsdl:operation name="Enroll">): adiciona um novo indivíduo ou uma nova "situação" para o sistema. Pode incluir diretamente ou depender de uma identificação positiva/negativa. Pode se utilizar de outros serviços primitivos de BIAS tais como criar indivíduo, definir dados biométricos, adicionar indivíduo em uma galeria, etc.
- Identificar (<wsdl:operation name="Identify">): executa uma função de identificação (1:N) de acordo com exigências e/ou recursos (por exemplo, pesquisar em várias galerias) do sistema. Pode se utilizar de outros serviços primitivos de BIAS tais como identificar indivíduo, definir dados biográficos, definir dados biométricos, etc.
- Verificar (<wsdl:operation name="Verify">): executa uma pesquisa 1:1 de acordo com exigências e/ou recursos de sistema. Pode se utilizar de outros serviços primitivos de BIAS tais como verificar indivíduo, definir dados biográficos, definir dados biométricos.
- Recuperar informações (<wsdl:operation name="RetrieveInformation">): recupera informações solicitadas sobre um indivíduo. Pode incluir dados biométricos, biográficos e/ou de múltiplas "situações". Pode se utilizar de outros serviços primitivos de BIAS tais como recuperar dados biográficos e/ou recuperar dados biométricos.

Obs.: Lembramos que para execução de capacidades de serviços compostos / de processo / de tarefa complexa se faz necessária que toda mensageria de todas as capacidades que estão sendo realizadas nos serviços que a compõem devem compreender a mensageria do serviço de processo em si.

e) Serviços para Atender as Respostas de Requisições Assincronas (*Pooling*).

- Pega Resultados do Cadastramento segundo Token (<wsdl:operation name="GetEnrollResults">):
- Pega Resultados de Identificação segundo Token (<wsdl:operation name="GetIdentifyResults">):
- Pega Resultados de Identificação de Indivíduos segundo Token (<wsdl:operation name="GetIdentifySubjectResults">):
- Pega Resultados de Verificação segundo Token (<wsdl:operation name="GetVerifyResults">):

f) Serviços Adicionais.

- Algoritmos e Funcionalidades Oferecidas pelas Capacidades de Serviços (<wsdl:operation name="QueryCapabilities">): retorna as funcionalidades que as capacidades / operações de serviços implementam, tais como os algoritmos de classificação utilizados, entre outros.

Porém, mesmo que a estrutura descrita se apresente funcional e cumpra os requisitos mínimos necessários para atender os processos de identificação por deduplicação de cidadãos e autenticação do indivíduo (sem nenhum processo adicional de operacionalização de cartões, resposta de informações gerenciais, etc), a proposta como exposta estabelece a construção de serviços com alta concentração de lógica agnósticas e não-agnósticas que fragilizam o reuso de serviços específicos com lógica puramente agnósticas. Tanto o é que o descritor WSDL sugerido é de um serviço somente com todas as capacidades elencadas contidas dentro do mesmo.

Ainda, esses serviços, por agregar lógicas em um único ponto, supõem a construção de componentes com grande extensão de código, o que impacta sobremaneira no uso de uma infraestrutura leve e escalável.

Por fim, a definição de capacidades que realizam muitas operações, e assim, com possível alta vinculação entre recursos de infraestrutura (e.g. acesso a diversas tabelas), afeta fundamentalmente o princípio de autonomia dos serviços, no qual o uso massivo de uma tabela por uma capacidade específica aumenta a latência de uso da mesma por outras capacidades de serviço.

NOTA:

a) Por questões de padronização e interoperabilidade, os serviços elementares a serem apontados neste documento terão seus nomes e suas capacidades compatibilizados com os apontados no documento "*Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0*", da OASIS, ou qualquer outra referência suplementar ao mesmo, em todos os capítulos seguintes deste documento. Assim, as capacidades de serviços serão documentadas como o padrão especifica: na língua inglesa.

b) Visto atender ao princípio já exposto anteriormente de contratos concorrentes, as capacidades serão estabelecidas em um único contrato, como apontados no documento "*Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0*", bem como deverão ser isoladas em contratos concorrentes de acordo com os grupos de serviços também já expostos anteriormente. Assim, os perfis das capacidades candidatas serão definidos unitáriamente, sendo seu agrupamento em serviços candidatos relacionados a seguir no Tópico a seguir neste documento.

6 PERFIL DOS CANDIDATOS DE CAPACIDADES E DOS SERVIÇOS

Para maiores detalhes do perfil de candidatos de serviços e principalmente suas mensagens de entrada e saída, sugerimos a leitura dos padrões da NIST definida nos arquivos de contrato de serviços BIAS.wsdl e de esquema de dados em CBEFF.xsd.

6.1 Serviços de Autenticação

Refere-se fundamentalmente ao atendimento dos princípios de autenticação através de recursos de identificação, pesquisa e validação do acesso a partir de chaves do RIC.

Capacidade	**Validar**
Capacidade OASIS	***Verify***
Contexto Funcional	Identifica única e inequivocamente um registro no RIC.A mensageria de retorno informa apenas esta validade (S/N).
Mensagem de Entrada	*VerifyRequestMessage*
Mensagem de Saída	*VerifyResponseMessage*
Característica de Acesso	Alto volume de acesso de leitura
Volumetria/SLA	10.000 registros/dia
Observações	Os elementos de dados de entrada *IdentityClaim* e/ou *ReferenceBIR* são parâmetros de identidade necessários.

Capacidade	**Identificar**
Capacidade OASIS	***Identify***
Contexto Funcional	Lista os prováveis elementos identificados em uma pesquisa nos registros do RIC (*Candidate*). A mensageria de retorno é a lista de dados básicos de pesquisa no RIC. Os dados básicos são limitados pela característica de acesso público.
Mensagem de Entrada	*IdentifyRequestMessage*
Mensagem de Saída	*IdentifyResponseMessage*
Característica de Acesso	Médio volume de acesso de leitura
Volumetria/SLA	100.000 registros/dia
Observações	Essa capacidade é implementada como um serviço síncrono, o sistema de execução processa imediatamente a requisição e devolve os resultados do parâmetro *ReturnData*.

6.2 Serviços de Federação

Refere-se fundamentalmente ao acesso através de chaves que garantam a federação na execução de processos dentro do ecossistema RIC. Envolve conceitos de Identidade Federada e uma implementação em uma arquitetura suplementar adjacente (logo não é classificado como um serviço interno ao modelo de serviços do RIC). Este modelo suplementar ora se utiliza da capacidade de Validação dos grupos de serviços de autenticação. Suas definições são parte integrante das documentações criadas pelo grupo de estudo de Federação de Serviços.

6.3 Serviços de Registro

Refere-se ao processo geral de criação, remoção e expiração da chave primária do RIC. Assim, o processo de cadastramento de uma nova identificação, é utilizado em uma composição com esse serviço para realizar todo o cadastramento. Não serão serviços diretamente disponíveis aos sistemas-clientes do RIC em geral.

Capacidade	**Criar**
Capacidade OASIS	**---**
Contexto Funcional	Cria uma chave única e inequívoca no registro no RIC.
Mensagem de Entrada	*EnrollRequest*
Mensagem de Saída	*ReturnData*
Característica de Acesso	Alto volume de acesso de gravação
Volumetria/SLA	400.000/dia
Observações	Como essa capacidade é processada de forma assíncrona, o sistema de execução retorna um *token* no parâmetro *ReturnData* que se refere ao protocolo de execução do pedido junto ao processo de deduplicação. Na consecução desta realização, o serviço *GetEnrollResults* é usado para sondar os resultados das requisições em processamento para dar entendimento que o processo já foi realizado.

Capacidade	**Apagar**
Capacidade OASIS	**---**
Contexto Funcional	Apaga uma chave única no registro no RIC tratando sua existência e realizando um processo assíncrono de informação de apagamento de todas as referências a mesma.
Mensagem de Entrada	*VerifyRequestMessage*
Mensagem de Saída	*ReturnData*
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	Esporádico
Observações	Como essa capacidade é processada de forma assíncrona, o sistema de execução retorna um *token* no parâmetro *ReturnData* que se refere ao protocolo de execução do pedido junto ao processo de deduplicação. Na consecução desta realização, o serviço *GetEnrollResults* é usado para sondar os resultados das requisições em processamento para dar entendimento que o processo já foi realizado.

Capacidade	**Atualizar**
Capacidade OASIS	**---**
Contexto Funcional	Atualização de dados biográficos (para uso do cidadão)
Mensagem de Entrada	*EnrollRequest*
Mensagem de Saída	*ReturnData*
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	10.000/dia
Observações	Esta capacidade unicamente atualiza dados biográficos, sendo tratado de forma síncrona.

Capacidade	**Expirar**
Capacidade OASIS	**---**
Contexto Funcional	Marca como inativa uma chave única e inequívoca no registro no RIC.
Mensagem de Entrada	*VerifyRequestMessage*
Mensagem de Saída	*ReturnData*
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	Esporádico
Observações	

6.4 Serviços de Cadastramento

Refere-se fundamentalmente aos serviços que atendem a manutenção da base do RIC e a respectiva entrega de informações como serviço (dados como serviço – DaaS). Junto aos serviços de cadastramento e informação encontra-se capacidade (ou serviço específico) para atender ao processo de agendamento de cadastramento que sugerimos ser suportada por base de dados distinta, mas integrada ao RIC.

Capacidade	**Cadastrar**
Capacidade OASIS	***Enroll***
Contexto Funcional	Permite o cadastramento (inclusão) na base de dados do RIC.
Mensagem de Entrada	*EnrollRequest*
Mensagem de Saída	*ResponseData*
Característica de Acesso	Alto volume de acesso de gravação
Volumetria/SLA	400.000/dia
Observações	

Capacidade	**Informar**
Contexto Funcional	Solicita permissão de acesso em nível de confidencialidade específico ao RIC.
Mensagem de Entrada	*BIASIdentity*
Mensagem de Saída	*ResponseData*
Característica de Acesso	Alto volume de acesso de leitura
Volumetria/SLA	10.000/dia
Observações	

Capacidade	**Atualizar**
Capacidade OASIS	***UpdateSubject***
Contexto Funcional	Permite a atualização na base de dados do RIC.
Mensagem de Entrada	*EnrollRequest*
Mensagem de Saída	*ReturnData*
Característica de Acesso	Alto volume de acesso de gravação
Volumetria/SLA	10.000/dia
Observações	

Capacidade	**Expirar**
Capacidade OASIS	***UpdateSubject (BiographicInfo.status=NOK)***
Contexto Funcional	Permite o cancelamento lógico no RIC, o que invalida as ações nos serviços de autenticação no RIC. Esta exclusão é lógica, não envolvendo a deleção de dados no RIC. A mensageria de retorno informa apenas a validade dessa ação (S/N).
Mensagem de Entrada	*EnrollRequest*

Mensagem de Saída	*ReturnData*
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	Esporádico
Observações	

Capacidade	**Cancelar**
Capacidade OASIS	***DeleteSubject***
Contexto Funcional	Realiza o cancelamento físico no RIC, eliminando a existência da instância associada a chave do RIC. A mensageria de retorno informa apenas a validade dessa ação (S/N).
Mensagem de Entrada	*BIASIdentity*
Mensagem de Saída	*ResponseData*
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	Esporádico
Observações	

6.5 Serviços de Informação

Refere-se fundamentalmente aos serviços que suportam o atendimento de terceiros no acesso a dados e situações no RIC. Ainda não é possível o desenvolvimento da total expectativa de capacidades bem como a apropriação dos aspectos tecnológicos necessários, porém este documento já aponta capacidades consideradas elementares para esse serviço

Capacidade	**Recuperar Dados Biográficos**
Contexto Funcional	Realiza a recuperação de dados biográficos de um indivíduo. Realiza preliminarmente um teste de validação desse indivíduo na base.
Mensagem de Entrada	*BIASIdentity*
Mensagem de Saída	*ResponseData*
Característica de Acesso	Alto volume de acesso de leitura
Volumetria/SLA	10.000/dia
Observações	

Capacidade	**Recuperar Dados Biométricos**
Contexto Funcional	Realiza a recuperação de dados biográficos de um indivíduo. Realiza preliminarmente um teste de validação desse indivíduo na base.
Mensagem de Entrada	*BIASIdentity*
Mensagem de Saída	*ResponseData*
Característica de Acesso	Baixo volume de acesso de leitura
Volumetria/SLA	1.000/dia
Observações	

6.6 Serviços de Integração

Refere-se a serviços que serão utilizados por soluções do RIC para solicitação de informações externas ao ambiente do mesmo. Envolve padrões de mensageria do tipo requisição-resposta oriundas do ambiente do RIC.

Capacidade	**Verificar**
Contexto Funcional	Atua verificando informações a partir de fontes confiáveis adjacentes.
Mensagem de Entrada	dadoPesquisaRIC
Mensagem de Saída	dadosRIC
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	SEM PREVISÃO
Observações	Tem como clientes potenciais cartórios, etc.

Capacidade	**Homologar**
Contexto Funcional	Suporta o registro de informações oriundas de fontes confiáveis junto ao RIC. Usando esses serviços, sistemas correlatos de terceiros podem atualizar informações que não sejam biométricas junto a base de dados do RIC.
Mensagem de Entrada	dadoPesquisaRIC
Mensagem de Saída	dadosRIC
Característica de Acesso	Baixo volume de acesso de gravação
Volumetria/SLA	SEM PREVISÃO
Observações	Tem como clientes potenciais cartórios, etc.

6.7 Serviços de Comunicação

Refere-se a serviços de informação baseados em eventos oriundos do modelo proposto para informação intempestiva a sistemas suportados pelo RIC. Baseia-se fundamentalmente em processos de mensageria direcionada por eventos (*publish-subscribe*) e pré-estabelece a existência de qualquer modelo de MQ ou ESB junto ao RIC.

Capacidade	**Centralizar**
Contexto Funcional	Trazer automaticamente informações distribuídas ou descentralizadas para o RIC.
Input	*BIASIdentity*
Output	*ResponseData*
Característica de Acesso	Alto volume de acesso de leitura no modelo de mensageria *publish-subscribe*
Volumetria/SLA	SEM PREVISÃO
Observações	Tem como clientes potenciais bases regionalizadas.

Capacidade	**Sincronizar**
Contexto Funcional	Repassar automaticamente informações distribuídas ou descentralizadas do RIC para outras bases de dados associadas ao projeto.
Input	*BIASIdentity*
Output	*ResponseData*
Característica de Acesso	Alto volume de acesso de leitura no modelo de mensageria *publish-subscribe*
Volumetria/SLA	SEM PREVISÃO
Clientes Potenciais	Tem como clientes potenciais bases regionalizadas

6.8 Serviços de Atendimento

Refere-se fundamentalmente a serviços em todos os níveis que são utilizados no desenvolvimento de soluções baseadas na orquestração de processos para a atividade de agendamento no cadastramento do RIC, a saber.

- Agenda (Solicitar, Reagendar, Confirmar, Realizar).
- Cadastramento e Atualização (conjunto de serviços de tarefa que se utilizam do motor de orquestração do ESB/SOA para implementar uma solução que preveja os macroprocessos do Sistema RIC).

Para implementação desse modelo, sugere-se o uso de serviços básicos de gerenciamento e execução de processos de negócio baseados em tarefas orquestradas.

6.9 Serviços de Operacionalização

Refere-se fundamentalmente a serviços em todos os níveis que são utilizados no desenvolvimento de soluções baseadas na orquestração de processos para a atividade de operacionalização junto a terceiros da emissão de documento do RIC. Dada sua característica de uso por entidades externas ao ecossistema do Sistema RIC - como no caso as emissoras de documento do RIC - essas foram isoladas do grupo de serviços de Atendimento para tratamento dos aspectos específicos de segurança.

- Emissão do Documento do RIC (Geração de Lotes, Confecção, Entrega, Cancelamento).

6.10 Serviços de Auditoria

Refere-se fundamentalmente a serviços assíncronos que suportam todos mecanismos de registro de *log* e auditoria de atividades gerais do RIC.

- *Log* (Geração do RIC)
- Auditoria (Uso do RIC)
- “Problemas Graves”

Esses serviços podem ser supridos pelo suporte de infraestrutura subjacente de controle do Barramento Corporativo de Serviços - ESB.

6.11 Serviços de Sincronismo

Estabelece um grupo de serviços que permite um possível sincronismo de dados entre unidades regionalizadas do RIC. Essa extensão é uma situação provável, não estando estabelecidas ainda diretrizes que permitam a definição dessas atividades sistêmicas.

- (DE/IN) Bases Geodistribuídas.
- (PARA/OUT) Bases Geodistribuídas.

No conjunto de soluções de serviços de sincronismo, dependendo do tipo de escalabilidade e distribuição previsto para implementação do RIC, essas podem ser substituídas por modelos de sincronismo, replicação ou técnicas modernas de distribuição junto ao sistema gerenciador de armazenamento de dados.

Diversas soluções de armazenamento massivo de dados já preveem recursos de sincronismo e/ou distribuição para atender as questões de consistência eventual (*Eventual Consistency*) de suas arquiteturas de armazenamento.

6.12 Serviços Gerenciais

Refere-se a disponibilização de dados como serviço na forma de fonte de dados utilizáveis por modelos analíticos para suporte às soluções OLAP.

7 PADRÕES DE MENSAGENS DAS CAPACIDADES CANDIDATAS

Ainda, para que se dê suporte ao entendimento desse documento, o qual descreve e define as tipagens comuns a serem utilizadas no padrão de mensageria proposto para o modelo, faz-se necessário uma declaração formal e completa das estruturas de mensagens (*message parts* e *message types*). Em grande parte, essas definições se referendam na INCITS 442. O roteiro apresentado é completo e claro. Destaca-se a completude dessa descrição e as minúcias que tornam o modelo fortemente extensível (e.g. na mensagem *CheckQuality* consta campo específico - AlgorithmVendor) que permite identificar o fornecedor do algoritmo de qualidade utilizado para determinar o índice de qualidade.

Da relação completa das tipagens apresentadas, é importante que se realce as principais pelas suas declarações no sumário do capítulo citado em conjunto com o estudo de suas declarações, a saber.

a) ACESSO AOS SERVIÇOS.

- *LOG* (*GenericRequestParameters*, *ApplicationIdentifier*, *ApplicationUser Identifier*, *BIASOperationName*): conjunto de dados repassados a todas as mensagens de chamada de serviços para uso de registros de *log*, no que se refere à identificação da aplicação que está realizando a chamada (*ApplicationIdentifier*), ao usuário que está utilizando a aplicação (*ApplicationUserIdentifier*) e aos serviços quando chamados (*BIASOperationName*).
- CÓDIGO DE RESPOSTA (*BIASFaultCode* e *BIASFaultDetail*, *ResponseStatus, ReturnCode*): usado em capacidades de serviços que respondem alguma forma de sucesso ou não.
- RESPOSTAS ASSINCRONAS (*TokenResultType*, *TokenType*): estrutura de dados utilizada para geração de *tokens* para uso em respostas assíncronas.
- CAPACIDADES DE SERVIÇOS (*CapabilityListType*, *CapabilityName*, *CapabilityType*): identifica as capacidades oferecidas pelos serviços implementados, tais como o formato CBEFF utilizado, os tipos de dados

biográficos disponibilizados, o modelo de identificação, os tipos de *match*/ *score* utilizados, entre outros.

b) DADOS BIOGRÁFICOS E BIOMÉTRICOS.

- DADOS BIOGRÁFICOS (*BiographicDataItemType*, *BiographicDataSetType* , *BiographicDataType*): dados estruturados na forma de lista de itens classificados para registro de dados biográficos. Somente os dados de primeiro e último nome são obrigatórios. A estrutura de mensagens (*BiographicDataType*) garante a transferência de uma lista de tipos de itens de dados (*DataItem*), segundo padrão determinado (*DataSet*). A especificação sugere o uso de um modelo padronizado definido em: FBI-EFTS [EFTS], FBI-EBTS [EBTS-FBI], DOD-EBTS [EBTS-DOD], INT-I [INT-I], NIEM [NIEM], xNAL [xNAL], HR-XML [HR-XML].
- TIPO DE DADOS BIOMÉTRICOS (*BaseBIRType*, *BinaryBIR*, URI_BIR, XML_BIR): é a tipagem básica que define o formato dos dados (BIR), a qual está trafegando junto à mensagem. Apresenta uma série de valores herdados que podem ser binários (*BinaryBir*), rotas web (URI_BIR) ou dados no formato XML (XML_BIR) retratados na forma de um BaseEncoded64.
- DADOS BIOMÉTRICOS INTERNOS (*BiometricDataElementType*, *BiometricDataListType*): dados estruturados na forma de lista de itens classificados para registro de dados biométricos. Seus tipos e estruturas básicas para armazenamento são definidos pelo CBEFF-BIR.
- DADOS BIOMÉTRICOS DE TRANSFERÊNCIA (*CBEFF_BIR_ListType*, *CBEFF_BIR_Type*, *BIASBiometricDataType*): suporte a diversas estruturas de dados na forma de lista de itens classificados para transferência de amostras de dados biométricos entre os diversos equipamentos compatíveis com o formato CBEFF. O *BIASBiometricDataType* é a superestrutura que transfere o conjunto de amostras do tipo *CBEFF_BIR_Type* em *CBEFF_BIR_ListType*.

c) PARÂMETROS DE RESPOSTA A SERVIÇOS DE VERIFICAÇÃO (1:1).

- BIAS (*IdentifySubjectResultType*, *BIASIdentity*, *BIASIDType*): estruturas de dados de mensagens de resposta de processos de verificação.

d) PARÂMETROS DE RESPOSTA A SERVIÇOS de IDENTIFICAÇÃO (1:N).

- LISTA DE CANDIDATOS (*CandidateListResultType*, *CandidateListType*, *CandidateType*): estruturas de dados de mensagens, de resposta, de processos de identificação com dados do *id* único, dados biográficos (*BiographicData*) e dados biométricos (*BiometricData*). São também componentes dessas mensagens os parâmetros de *Score* e *Rank* para cada candidato.

e) PARÂMETROS DOS SERVIÇOS DE DEDUPLICAÇÃO.

- CLASSIFICAÇÃO (*Classification*, *ClassificationAlgorithmType*, *ClassificationData*): estrutura as informações sobre os resultados de classificação e o algoritmo utilizado para determinar a classificação.
- FUSÃO (*EncounterListType*, *FusionDecision*, *FusionInformationListType*, *FusionInformationType*, *FusionResult*, *FusionScore*): representa as informações necessárias para realizar operações de fusão, principalmente no que se refere a identificação do modelo de decisão de *match* que é definida por um algorítmo de *matching*.
- MATCH (*VendorIdentifier*, *ProductID*, *MatchType*, *Score*, *QualityData*, *ListFilterType*): a estrutura de dados da resposta do processo de *match*.
- SERVIÇOS COMPOSTOS (*ProcessingOptionsType*): define um parâmetro para definir a realização de uma sequência de atividades de processamento.

Note-se que o modelo de mensagens proposto adiciona o princípio de grupos de usuários, nos quais o usuário pode ser cadastrado. O documento define como Galeria (*Gallery*) ou Grupo da População, indexando esse grupo pelo seu *GalleryID*. Este enfoque do modelo adiciona a possibilidade de *clusterização* dos grupos populacionais.

8 MODELO TECNOLÓGICO PARA ATENDER OS SERVIÇOS DO RIC

Para dar entendimento aos perfis de grupos de serviços apresentados, a Figura 10 ilustra os prováveis modelos de mensageria previstos para o RIC (à exceção do processo de deduplicação), ao qual iremos usar como base para tratar a associação do tipo de mensagem e os grupos de serviços.

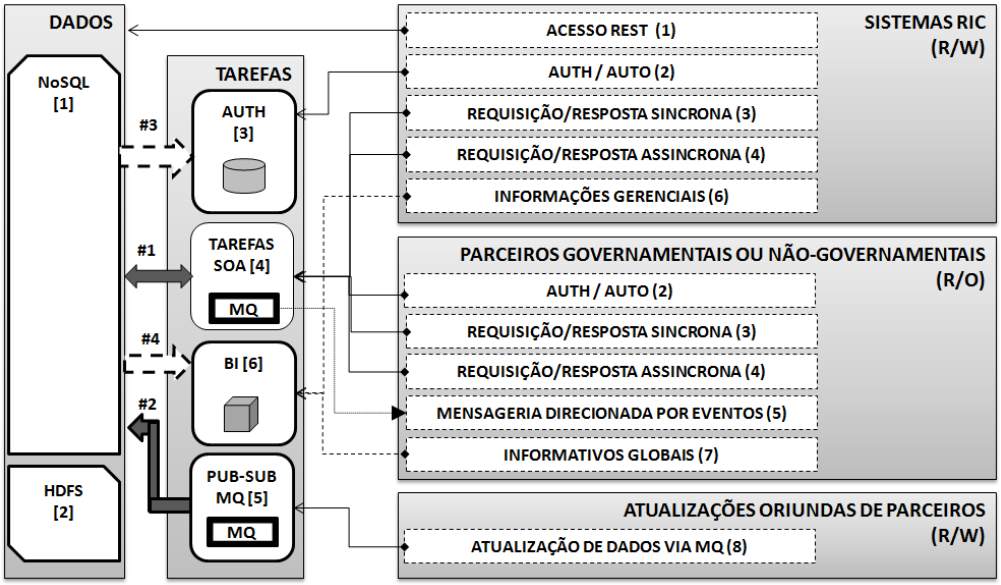


Figura 10 - Esquema Geral Proposto

8.1 Dos Elementos Tecnológicos Sugeridos (notação [])

[1] Uma arquitetura de armazenamento massivo de dados, que utilize técnicas de consistência eventual e que permita a implementação de bases de dados distribuídas, escaláveis com alta performance e baixa latência.

[2] Uma arquitetura de armazenamento massivo de arquivos, que utilize técnicas de consistência eventual e redundância, que permita a implementação de processos de mapeamento e redução na distribuição no armazenamento dos originais digitais de digitais, faces, íris e assinatura [3]

[4] Uma arquitetura de Barramento Corporativo de Serviços com um *Message Queue* (MQ) que aplique padrões de mensageria confiável, de enfileiramento assíncrono, de implementações redundantes de serviços e de contratos SOA concorrentes, e que possibilite a implantação do mensageria baseada em eventos (pub/sub).

[5] Uma arquitetura independente com um *Message Queue* (MQ) que aplique padrões de mensageria confiável, de enfileiramento assíncrono, de implementações redundantes de serviços e de contratos SOA concorrentes, e que possibilite a implantação do mensageria baseada em eventos (pub/sub), com requisitos restritos de segurança e confiança computacional.

8.2 Dos Modelos de Mensageria Permitidos (notação: ( ))

(1) Acesso REST: acesso exclusivo e restrito a funcionalidades de CRUD diretamente sobre o modelo de dados do RIC. Este acesso será utilizado somente por funcionalidades específicas e restritas dentro do Sistema RIC.

(2) AUTH: modelo de comunicação direta dentro do ESB aos dados básicos válidos ao perfil de serviços de Autenticação.

(3) Modelo de Requisição-Resposta Síncrono: modelo de mensageria no qual a aplicação requisitante encaminha uma mensagem de requisição (*request*) e imediatamente suspende o seu processamento no aguardo de uma mensagem de resposta (*response*). Mensagens de falhas (*message faults*) são previstas para indicar situações imprevistas ou de indisponibilidade dos serviços.

(4) Modelo de Requisição-Resposta Assíncrona (com suporte de MQ): modelo de mensageria no qual a aplicação requisitante encaminha uma mensagem de requisição (*request*) e não suspende o seu processamento. Essas requisições são empilhadas em filas para processamento (*messages queues*) que terão como função adicional reencaminhar uma mensagem de resposta. Assim, a grande vantagem que MQ de mensagem assíncrona pode delegar um pedido nós diferentes, escaláveis e balanceados. Ele pode redirecionar os pedidos entre computadores segundo uma análise de carga a fim de suportar o processamento massivo de mensagens. Quando o pedido é concluído, o próprio computador que processou a mensagem pode retornar a resposta diretamente para o terminal de origem da mensagem. Mensagens de falhas (*message faults*) são previstas para indicar situações imprevistas ou de indisponibilidade completa dos serviços.

(5) Modelo de mensageria baseada em eventos (com suporte do MQ): modelo de

pub/sub, utilizando o MQ presente no ESB.

(6) Acesso a relatórios gerenciais pré-definidos.

(7) Acesso a serviços de BI com recursos de disponibilização de relatórios pré-definidos, consultas *ad-hoc* e suporte ao acesso a análise multidimensional.

(8) Modelo de MQ independente com suporte a mensageria baseada em eventos com fortes requisitos de segurança.

8.3 Dos Fluxos de Dados Entre Camadas (notação: setas largas escuras)

- Fluxo #1 de acesso a camada de dados: acesso das tarefas síncronas e assíncronas em (3), (4) e (5), atualizando o modelo de dado. Esse fluxo se refere às atualizações oriundas do Sistema RIC, ou de consulta tanto do Sistema RIC quando de requisições (R/O) dos sistemas de parceiros privados (não-governamentais).
- Fluxo #2 de atualizações restritas: acesso das requisições de atualização dos modelos de dados com tratamento intensivo de validade, prioridade e auditoria por se tratar de atualizações oriundas de requisições (R/O) dos sistemas de parceiros privados (não-governamentais).

8.4 Dos Fluxos de Consistência Eventual (notação: setas largas tracejadas)

- Fluxo #3 de consistência eventual ao armazenamento chave-valor para suporte aos processos de Validação.
- Fluxo #4 de consistência eventual dos Cubos Multidimensionais (ETL).

9 DETALHES DO PROCESSO DE CADASTRO E DEDUPLICAÇÃO

9.1 Introdução

O conceito de deduplicação refere-se ao processo de examinar, durante o procedimento de cadastramento, se a amostra biométrica que está sendo cadastrada tem alguma amostra correspondente em todo o banco de dados já existente. Desta forma, a amostra é comparada as "N" amostras já cadastradas, uma a uma. Se existe alguma amostra correspondente, o indivíduo não é cadastrado, e, portanto, não recebe uma nova identidade a fim de evitar uma entrada duplicada. Caso não exista amostra correspondente, o usuário é cadastrado de forma correta e um número único é associado à amostra apresentada pelo individuo (DECANN, 2013).

O processo de deduplicação é necessário para garantir que todos os indivíduos da população tenham apenas um único número no banco de dados. Por exemplo, uma entrada duplicada pode ser criada intencionalmente por um impostor para futuramente fraudar o sistema e obter algum benefício utilizando a identidade de outro indivíduo.

O processo de deduplicação vem ganhando notoriedade e atenção nos últimos anos, devido particularmente a programas de identificação civil de grande escala como o caso da Índia, México e Indonésia, em que enormes bases de dados precisam garantir a unicidade dos indivíduos cadastrados.

A deduplicação também pode ser considerada um processo de identificação, no qual é feita uma comparação 1:N. Entretanto, para cada indivíduo que está sendo cadastrado, é realizada uma comparação, o que exige alto poder de processamento do sistema. Como exemplo da complexidade dessa operação, a Índia cadastra, diariamente, 1 milhão de indivíduos, os quais são comparados com os 650 milhões já cadastrados, gerando mais de 500 trilhões de comparações por dia.

9.2 Cadastro e Deduplicação no Sistema RIC

No que se refere ao Serviço de Cadastramento do RIC, um fluxo assíncrono, suportado por mensageria confiável, remete as informações cadastrais as bases do modelo de armazenamento do RIC e para a entidade deduplicadora para geração e

solicitação de incorporação as bases do RIC de um novo registro (com a intempestiva geração do número do RIC).

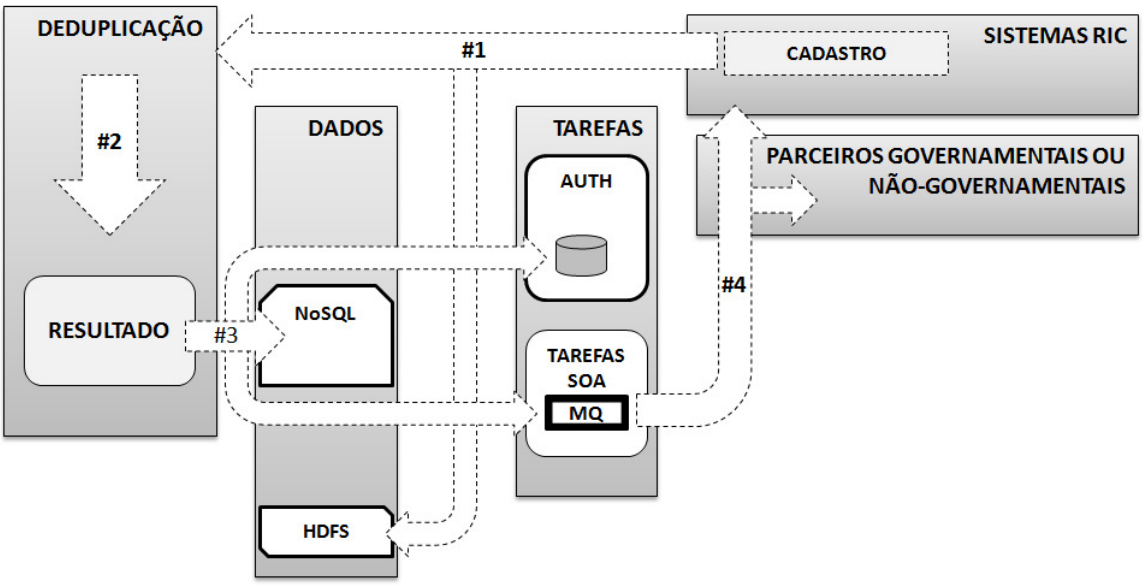


Figura 9 - Fluxo de Dados e Mensagens dos serviços de Cadastro / Atualização

Do modelo ilustrado na Figura 9 temos os seguintes fluxos previstos.

- **Fluxo #1**: repasse de informações massivas (imagens) ao modelo de armazenamento de dados do RIC em conjunto com o repasse das informações biométricas a entidade deduplicadora. Essas informações (biométricas e de cadastramento) são encaminhadas associadas com respectivas informações de trilha de auditoria (quem solicita - autorização, de onde - endereço MAC, com que valor de vetor de hora - *vector timestamp*) e, fundamentalmente, com o número de protocolo gerado especificamente com um código *hash* dos dados de auditoria para associação futura com os dados encaminhados às bases de armazenamento do RIC.
- **Fluxo #2**: realização da deduplicação das imagens em *templates*, suportada por enfileiramento confiável e assíncrono das solicitações.
- **Fluxo #3**: após o exaustivo processo de deduplicação (Fluxo #2), é encaminhado associado com o código *hash* do protocolo (gerado para o Fluxo #1) para registro dos *templates* nas bases de dados do RIC. Somente

esse encaminhamento poderá registrar os *templates* nessa base.

- **Fluxo #4**: ao final do processo, isto é, depois de dada uma garantia de seu encerramento efetivo, é atualizada a base de chaves e valores dos Serviços de Autenticação (armazenadores *in-memory*) que está posicionada junto aos componentes do Barramento de Serviços Corporativos, e é gerado o evento de GERAÇÃO DO NÚMERO DE RIC junto aos serviços de pub/sub existentes no barramento para geração de mensagem de notificação aos Sistemas de Cadastramento do RIC e aos parceiros governamentais e privados assinantes do serviço de pub/sub.

10 RELAÇÃO ENTRE O ESQUEMA E OS SERVIÇOS

10.1 Autorização

Como é premissa que serviços SOA atendam a requisitos técnicos de composição, todos os serviços projetados para atendimento do RIC devem estabelecer um acoplamento inicial ao processo de autorização (especificamente à uma capacidade de validação).

Esse processo e o esquema para ele idealizado prevê que esses serviços não mantenham estados (*stateless*), sejam extremamente atômicos (outras estruturas devem ser utilizadas para manutenção de estado e de contexto) e seja suportado por modelos de armazenamento de baixíssima latência (no caso, *in-memory* dos pares de chaves/ número do RIC e valores/*templates* biométricos). Além disso, para garantir a disponibilidade efetiva desse serviço, o modelo de armazenamento a ser idealizado deverá estar presente junto ao Barramento de Serviços Corporativo para acesso direto pelo mesmo.

Isto posto, percebe-se que haverá uma Consistência Eventual entre o modelo de armazenamento de dados do RIC e esse conjunto de soluções para alta disponibilidade dos serviços, sendo que a oportunidade dessa eventualidade - já que somente é afetada por um cadastro ou atualização de dados biométricos - já é ofertada pelo longo tempo de processamento para deduplicação das mesmas.

10.2 Registro e Cadastro

Esses grupos de serviços, além de tratar do armazenamento dos dados biográficos e biométricos impõem outras características e tarefas agregadas, a saber:

- tratamento do tempo de resposta devido à transferência massiva de dados oriunda dos aplicativos clientes;
- encaminhamento coordenado de dados junto a infraestrutura de dados do RIC e a infraestrutura de deduplicação, garantida por uma chave temporária de processo de RIC (status de "em geração de número RIC");
- garantia de acesso restrito oferecida pela infraestrutura subjacente de gestão de identidades federadas.

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços, descritas a seguir.

- Coleta de dados biográficos e biométricos do cidadão *off-line*.
- Processamento de dados biográficos e biométricos do cidadão *off-line*.
- Verificação dos dados biográficos e biométricos coletados.
- Registro de informações (número RIC, minúcias, dados biográficos).
- Requisição da individualização biométrica do cidadão AFIS/DPF (encaminhamento coordenado de dados junto a infraestrutura de dados do RIC e a infraestrutura de deduplicação) - que se dá de forma automática pela aplicação cliente.
- Cancelamento da solicitação de emissão do Documento RIC.
- Rotina para expirar o Documento RIC.

10.3 Informação e Integração

Esses dois modelos baseiam-se no princípio básico de mensageria requisição-resposta, considerada suas duas origens: a infraestrutura de serviços RIC solicitando informações de entidades parceiras, ou o acesso por organizações governamentais e não-governamentais, apenas para leitura de informações existentes no armazenamento do RIC.

As solicitações oriundas do RIC são empilhadas em uma fila de requisições, suportada por dinâmica de mensageria confiável, o que imputa que os parceiros do modelo implementem algum tipo de mecanismo de consulta a esses dados solicitados como serviço. Não haverá nenhuma cobrança de garantia de entrega de informações pelos parceiros, sendo imposto a fila o suporte a um mecanismo de tentativas tempestivas o caso de falha nos parceiros.

As solicitações aos serviços do RIC se dão de forma síncrona ou assíncrona, diretamente aos serviços do RIC, estando o solicitante devidamente registrado no serviço de identidade federada para tal fim.

Do levantamento original do sistema, foram observadas como funcionalidades básicas

do CANRIC e apontadas para serem oferecidas por esse grupo de serviços, a saber.

- Disponibilidade de serviços para interoperação com os sistemas de Órgãos de Identificação (requisição do Sistema RIC).
- Disponibilidade de serviços para interoperação com os sistemas de Órgãos de Identificação (requisição de um Parceiro).
- Histórico de dados biográficos e biométricos do cidadão.

10.4 Comunicação

Modelo de processos de mensageria direcionada por eventos (*publish-subscribe*), gerenciados pelo ambiente RIC e acionado por ocorrências específicas nos seus dados armazenados (ex.: extinção de RIC por falecimento). Esse modelo será suportado por arranjos tecnológicos entre os gestores do RIC e definidos parceiros governamentais ou não governamentais para encaminhamento de uma mensagem de notificação para esses com garantia de entrega (algum suporte de mensageria confiável). É importante que esse modelo registre consistentemente a informação que a mensagem foi entregue corretamente e em tempo aos parceiros assinantes (*subscribers*).

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços:

- notificação de problemas nos dados de solicitação de emissão do RIC.

10.5 Atendimento

Para implementação desse modelo, sugere-se o uso de serviços básicos de gerenciamento e execução de processos de negócio baseados em tarefas orquestradas junto a motores de execução BPM/BPEL providas por plataformas profissionais de SOA.

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços as que serão descritas a seguir.

- Criação e manutenção da agenda de atendimentos dos Postos de Identificação.
- Agendamento da solicitação de emissão do RIC.
- Cancelamento do agendamento da solicitação de emissão do RIC.

10.6 Operacionalização

Para implementação deste modelo sugere-se o uso de serviços básicos de gerenciamento e execução de processos de negócio baseados em tarefas orquestradas junto a motores de execução BPM/BPEL providas por plataformas profissionais de SOA.

Especificamente para os serviços de operacionalização, é observado que diversas de suas capacidades devem ser implementadas pela execução, ao nível do sistema operacional, através de rotinas em "*batch*".

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços as seguintes.

- Registro de informações de controle de solicitações de emissão do RIC e do Documento RIC.
- Registro de envio/recebimento do arquivo ao fornecedor de impressão/ personalização do Documento RIC.
- Geração do lote de números tipográficos do Documento RIC (número de suporte).
- Registro de recebimento das remessas contendo os Documentos RIC confeccionados.
- Registro de informações do certificado digital emitido pela AC.
- Requisição de emissão e/ou revogação do certificado digital a AC.
- Entrega do Documento RIC (*on-line* e *off-line*).

10.7 Auditoria

Como um elemento presente nos Barramentos de Serviços Corporativos, pressupõem-se o uso do processo de Monitoramento de Atividades do Negócio - BAM, em conjunto com os padrões de mensageria unidirecionais BAM, na automatização das capacidades de registros de trações de *log* e na formação de saídas para controle da capacidade e desempenho do sistema.

Assim, esses serviços podem ser supridos pelo suporte de infraestrutura subjacente (Barramento Corporativo de Serviços - ESB) em modelos de filas unidirecionais no *middleware* (*Notify Services by Unidirectional Queuing*). Nesse caso, mensagens

unidirecionais serão geradas de forma a possibilitar aos modelos de serviços dos RIC (como um todo) de capacidades de arquivamento e auditoria. Adicionalmente, *triggers* e/ou serviços *publish-subscribe* devem ser implementados visando atuar após o registro desses eventos em situações ocasionais de identificação - por máquina - da ocorrência de atividades não autorizadas (observada durante o processo de registro de auditoria).

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços:

- registro do *login* de operações realizadas pelo usuário do sistema.

10.8 Sincronismo

Estabelece dois grupos de serviços para sincronismos de dados (de e para) de forma a atender quaisquer solicitações de sincronia a determinados dados ou recursos digitais (imagens de digitais, faces, íris e assinaturas) entre o RIC e seus parceiros regionais. Ainda não existem maiores detalhes que possam ser tratados essas realizações.

10.9 Gerencial

Refere-se às atividades voltadas a disponibilização de serviços de acesso a cubos multidimensionais, tratando dos assuntos:

- dos banco de dados (em memória) dos cubos multidimensionais;
- da consistência eventual desses cubos multidimensionais por processo de
- da permissão de acesso a dados globalizados para parceiros e outros
- da permissão de acesso ao Sistema RIC-BI que prevê com recursos/saídas:
  - Relatórios Formatados: de acesso periódico ou intempestivo, podendo ser acessado pelo usuário ou encaminhado diretamente (anexos de email).
  - Consultas *Ad-hoc*: criadas sob demanda especificamente com conteúdo, *layout* ou cálculo necessário e que podem agilizar ou facilitar uma tomada de decisão pontual.
  - Análise Multidimensional: suportado diretamente pelo uso de ferramentas OLAP, permite ao usuário interagir com o resultado através de processos de análise utilizando-se de operações multidimensionais (*drills, pivot*, etc.).

Em geral, o analista opera buscando situações de:

- analisar dados contextualizados;
- dar suporte ao trabalho com hipóteses; e/ou
- procurar relações de causa e efeito.

Do levantamento original do sistema, foram observadas como funcionalidades básicas do CANRIC e apontadas para serem oferecidas por esse grupo de serviços:

- disponibilização de consultas e relatórios gerenciais na Base Nacional do Registro de Identificação Civil.

10.10 Modelagem Canônica de Dados

Entendemos que a troca de mensagens, seu modo de transmissão e a semântica são partes fundamentais em sistemas distribuídos, pois são a única maneira que os componentes de uma arquitetura orientada a serviços possuem de se comunicar e sincronizar suas ações.

Mesmo reconhecendo que os esquemas canônicos representem uma visão *front-end* do modelo de dados - pois eles existem para definir conceitos e agir como mediadores ideais - o que se idealiza é que o arquétipo de armazenagem de dados seja par-a-par com a Modelagem Canônica da Mensageria que será usada como base dos modelos de mensagens utilizados na troca interoperável de dados entre o RIC e os demais sistemas ou consultas existentes pelos sistemas externos através de terminais oficiais (*endpoints*). Isto facilitaria sobremaneira a recuperação e o encaminhamento dos resultados, nos quais os terminais dos serviços (expressos pelas suas capacidades) não implementem nenhuma lógica que agregue latência aos resultados de consultas ao RIC.

Porém, mesmo sugerindo esse acoplamento entre modelo de dados e mensageria, este trabalho desacopla o desenvolvimento da semântica do modelo de mensageria do projeto de serviços de forma a garantir uma independência entre dados e capacidade dos serviços a serem projetados durante a etapa de análise, impondo um baixo acoplamento entre o fluxo de dados e os requisitos sistêmicos no projeto das capacidades candidatas de serviços.Do processo de modelagem canônica das mensagens (como estabelecido na literatura) e seus resultados finais, temos os seguintes padrões de projeto usuais.

- *Russian Doll*: é baseado na redução do tamanho do esquema da mensagem pela colocação de um esquema dentro do outro. O padrão de *Russian Doll* define todos os seus subelementos localmente, assim cada elemento e o seu tipo são encapsulados por elementos-pais. São considerados altamente dissociados (os elementos não são globalmente dependente em outros elementos) e coesos (os elementos são agrupados em um único elemento-pai independente). Este padrão sintetiza esquemas destinados a ter pouca interação com outros sistemas e sem reutilização dos seus componentes.
- *Salami Slice*: esse padrão já expõe o conteúdo dos modelos, pois são movidos todos os seus elementos definidos localmente em definições globais.

- *Venetian Blind*: esse estilo utiliza definições de tipo global para aumentar a reutilização das capacidades dos esquemas, porque todos os subelementos são localizados, ele vem com vantagem adicional de ser capaz de esconder os elementos dentro do espaço de nomes (namespaces). Esta abordagem permite que você exponha suas definições de estrutura para reutilização usando-se do *elementFormDefault* funcionando como um interruptor para ocultar ou expor todos os elementos no espaço de nomes (*namespaces*).
- *Garden of Eden*: assim como a abordagem *SalamiSlice,* esse modelo é modular e estruturado através da definição de todos os elementos a nível global. Como na abordagem *Venetian Blind*, nesse modelo todas as definições de tipo também são declaradas globalmente. Assim, cada elemento é definido globalmente como um filho imediato do nó (“<schema>”) e os tipo de elementos (atributos) podem ser definido como um dos tipos complexos nomeados globalmente.

Para o projeto efetivo dos serviços, nossa sugestão é o uso da abordagem de *Garden of Eden*, a qual implementa características da abordagem *Venetian Blind* com a *Salami Slice*. A vantagem dessa abordagem é que os esquemas são reutilizáveis, pois ambos os elementos e os tipos são definidos globalmente, e assim ambos estão disponíveis para reutilização. Neste sentido, essa abordagem oferece o máximo de conteúdo reutilizável.

10.11 Modelo Estrutural Básico

Figura 15 – Famílias de Colunas para o RIC e suas escalas de acesso

a) Armazenamento de Dados do RIC

- Determinante

  NÚMERO DO RIC

  UF DE CADASTRO

  DATA DE CADASTRO

- Biográficos

  No que se refere a transferência de dados biográficos, lembramos que a modelo canônico de dados de biografia prevê que cada implementação (organização) preveja uma lista definida pela mesma de BiographicDataItemType de elementos dos tipo *BiographicDataElements.*

Para execução da Prova de Conceito, e segundo o RT Execução de Prova de Conceito, temos como campos:

- NOME COMPLETO;
- DATA DE NASCIMENTO;
- SEXO;
- FILIAÇÃO;
- NATURALIDADE;
- NACIONALIDADE;
- SIRC ou RG;
- DADOS DO CADASTRAMENTO (DATA, AUTOR);
- IMAGENS BIOMÉTRICAS;
- OUTRAS IMAGENS (FOTO, DOCUMENTO COMPROVATÓRIO, DOCUMENTO DE RESIDÊNCIA).

Lembramos que alguns desses dados podem ser obrigatórios ou não.

- Relacionamentos

  Uma lista de NÚMEROS DE RIC relacionados de forma a estabelecer um modelo de parentesco/responsável para usos futuros.

- Demográficos

  Estabelece uma lista de campos padronizados que tem como característica alta volatilidade e não-obrigatoriedade, a saber:

  - ENDEREÇO;
  - DADOS DE ACESSO A PESSO (EMAIL, TELEFONE).

Obs.: é provável uma implementação de acesso ao dados Demográficos pelo próprio cidadão na atualização dos dados dessa família de colunas.

b) Armazenamento de Dados para suporte ao RIC

- Auditoria

  Nota: todos os pacotes brutos recebidos devem ser mantidos como forma de garantir o não repúdio.

c) Armazenamento de Dados das Matrizes Digitais do RIC

- Imagens

  Nota: pacote de imagens PNG do processo *Tenprint* e das imagens de face no modelo de armazenamento de árvore de diretório.

11 CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da MJ/SEe da Universidade de Brasília, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas.

Como modelo para avaliação e sugestões, este produto não representa um produto finalístico, sendo provável sua revisão após ciclos de análise e reavaliação e, principalmente, quando do atingimento de resultados parciais na realização das atividades envolvidas no subprojeto de Ecossistema do RIC e das avaliações obtidas por meio de Provas de Conceito.

Porém, o resultado de uma primeira avaliação deste documento pode permitir o direcionamento inicial de uma Prova de Conceito (PoC) mínima visando nortear a avaliação de quesitos específicos de infraestrutura, tal como os produtos e ferramentas que suportam os modelos e arquétipos sugeridos, questões de desempenho e curvas de ruptura na entrega de serviços, identificação de requisitos mínimos de *hardware* de infraestrutura de armazenamento, entre outros. É fator fundamental dessa PoC também comprovar a eficácia e eficiência do modelo dada a capacidade de resposta de um o número de acesso previsto para o registro da totalidade de cidadãos.

Nesse sentido, este primeiro desenvolvimento deste Produto é importante, pois, minimamente, elementos gerados podem dar suporte em todos os demais RTs do projeto.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe da MJ/SE/RIC, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

12 REFERÊNCIAS

AADHAAR TECHNOLOGY & ARCHITECTURE - Principles, Design, Best Practices, & Key Lessons.

BHARGAV-SPANTZEL, A., CAMENISCH, J., GROSS, T., E SOMMER, D. User centricity: a taxonomy and open issues. Journal of Computer Security, 15(5), 493-527. 2007

DECANN, Brian; ROSS, Arun. De-duplication errors in a biometric system: An investigative study. In: Information Forensics and Security (WIFS), 2013 IEEE International Workshop on. IEEE, 2013. p. 43-48.ERL, T. Service-Oriented Architecture: Concepts, Technology, And Design. Editora Pearson Education, 2005. ISBN 813171490X, 9788131714904

JøSANG, A. e POPE, S. (2005). User centric identity management. In AusCERT Asia Pacific Information Technology Security Conference 2005.

JOSUTTIS, N. M. SOA na Prática. Tradução de Ivan Bosnic. 1. ed. Rio de Janeiro: Alta Books, 2008. 265 p. ISBN 978-85-7608-184-5.

LINTHICUM, D. Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide. Addison-Wesley, 2009. pg. 199

OASIS. "Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0". OASIS Standard. 24 May 2012.

PORTAL UIDAI. https://portal.uidai.gov.in/uidwebportal/dashboard.do

PROGRAMA RIC no RT de Soluções de Message Queue e Barramentos de Serviço Corporativos.

PROGRAMA RIC, RT Infraestrutura Tecnológica: Avaliação na Necessidade de Contratação de Múltiplos Parceiros.

TORRES, J.A.S., Diagnóstico Comparado do Governo Eletrônico Brasileiro - Uma Análise com Base na Estratégia de Gerenciamento de Identidades. Monografia – Especialização em Segurança da Informação e Comunicações. Instituto de Ciências Exatas - Departamento de Ciência da Computação – Universidade de Brasília, 2014.

UID Enrolment Proof-of-Concept Report. <http://www.biometrics.org/bc2011/presentations/Standards/0927_0930_Mr13_Tilton.pdf>

RT Políticas e Recomendações Técnicas e Operacionais para Protocolo de Comunicação Segura.

RT Soluções de Message Queue e Barramentos de Serviço Corporativos

RT Relatório Preliminar dos Inventários de Serviços de Identificação

RT Características e Questões de Pesquisa sobre Gestão de Identidades

RT Armazenamento Biométrico

Diagnóstico da Identificação Civil no Brasil

Um Estudo Comparativo de Estratégias Nacionais de Gestão de Identidades para Governo Eletrônico.

Diagnóstico do governo eletrônico brasileiro - uma análise com base no modelo de gerenciamento de identidades e no novo guia de serviços

Diretrizes de Interoperabilidade e Dados Abertos.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br– www.cdt.unb.br – www.latitude.eng.br