2012

Manual SDK Acesso

MCA – Módulo Controlador de Acesso

Manual de referência dos requisitos funcionais e não funcionais atendidos

Versão 1.1 - 20/04/2012

Sumário

1. Objetivos 8
2. Comandos 9
2.1. Carga de lista de permissão de faixa horária 9
2.2. Lista de feriados 9
2.3. Lista de liberação 9
2.4. Lista de templates biométricos 9
2.5. Comando de carga de lista de cadastro de pessoas 10
2.6. Lista de faixa horária de refeitório 10
2.7. Exclusão de lista 10
2.8. Status de lista 11
2.9. Mensagem do display 11
2.10. Inclusão de usuário biométrico (templates) 11
2.11. Exclusão de usuário biométrico (templates) 11
2.12. Atualização de firmware 12
2.13. Atualização para versão mais antiga 12
2.14. Evento de atualização 12
2.15. Comando de backup 12
2.16. Configuração do dispositivo 13
2.17. Atualização de data e hora 13
2.18. Comando de status 13
2.19. Comando de bloqueio e desbloqueio de dispositivo 14
2.20. Limpar arquivos de eventos 14
2.21. Ativar e desativar emergência 14
2.22. Ativar e desativar monitoramento de alarmes 15
2.23. Horário de verão 15
2.24. Ativar e desativar saída digital 15
2.25. Status de saída e entradas digitais 15
2.26. Mapa do Smart Card 16
2.27. Copiar arquivo de log 16
2.28. Processos automáticos 16
2.29. Comando não reconhecido 17
2.30. Consistência das informações 17
2.31. Log das informações 17
2.32. Tamanho das listas 17
2.33. Timeout de comandos 17
2.34. Execução do comando 17
2.35. Mensagem para aplicação das configurações 18

3. Configurações 19
3.1. Ativação do modo configuração 19
3.2. Informações configuradas 19
3.3. Confirmação da configuração 19
3.4. Correções de informações digitadas 19
3.5. Conferência das informações 20
3.6. Identificação do dispositivo 20
3.7. Bloqueio do teclado 20
3.8. Configurações necessárias 20
3.9. Permissões do dispositivo 21
3.10. Mapa Smart Card 21
3.11. Exibir configurações 21
3.12. Mensagem padrão 21
3.13. Configurar propriedades 21
3.14. Leitoras bloqueadas 22
3.15. Tratamento de conversões 22
3.16. Conectar com Servidor 22
3.17. Sincronismo de informações 22
3.18. Desligar saídas, sensores e display 23
3.19. Persistência das propriedades 23
3.20. Mensagem por evento 23
3.21. Exibição de data e hora 24
3.22. Horário de verão 24
3.23. Acionamentos de emergência 24
3.24. Funções 24
3.25. Tamanho de arquivos 25
3.26. Valores default 25
3.27. Duplicação de templates biométricos 25
3.28. Controle SAD 26
3.29. Leitora 26
3.30. Acionamentos da validação de acesso 26
3.31. RFID 26
3.32. Barras 26
3.33. SmartCard como proximidade 27
3.34. Acionamentos de alarme 27
3.35. Configurar por linha de comando 28
3.36. Utilização de DHCP 28
3.37. IP Fixo 28

3.38. Timeout de execução de comandos 29
3.39. Timeout do envio de eventos e requisições de acesso 29
3.40. Configurações de leitoras 29
3.41. Configuração da revista 29
3.42. Tipos de crachá 30
3.43. Acionamentos da revista 30
3.44. Restrições da configuração 30
3.45. Validação de autenticidade do BDCC por tipo de crachá 30
4. Validações 31
4.1. Validação de crachás do BDCC 31
4.2. Leitura dos dados gravados no crachá 31
4.3. Descriptografia dos dados de crachás do BDCC 31
4.4. Comparação de ID descriptografado com ID real 31
4.5. Ausência de campo no mapa do Smart Card 32
4.6. Atualização de pendências 32
4.7. Permissão 32
4.8. Situação 32
4.9. Afastamento 33
4.10. Crédito de acesso 33
4.11. Faixa horária do crachá 33
4.12. Crachá mestre 33
4.13. Exibição de mensagem 33
4.14. Senha 33
4.15. Intervalo mínimo de almoço 34
4.16. Interjornada 34
4.17. Autorização de entrada 34
4.18. Controle de Nível 35
4.19. Validade do crachá 35
4.20. Controle de Anti-dupla 35
4.21. Crachá com chave padrão 35
4.22. Crachá desatualizado 35
4.23. Atualizar somente crachás smart card 36
4.24. Autorizador 36
4.25. Revista aleatória 37
4.26. Quantidade de pessoas sorteadas 37
4.27. Revistados de forma imperativa 37
4.28. Acesso negado antes da revista aleatória 38
4.29. Controle SAD 38

4.30. Máscara do crachá 38
4.31. Identificador de uso do crachá 38
4.32. On-line / Off-line 39
4.33. Lista de liberação / bloqueio 39
4.34. Validação no DFS 39
4.35. Validação com entradas digitais associadas 39
4.36. Desistência de acesso 40
4.37. Tipo de pessoa 40
4.38. Burla de catraca 40
4.39. Tempo mínimo de permanência 40
4.40. Controles off-line para validação de acesso 40
4.41. Validação com biometria 1:1 41
4.42. Validação com biometria 1:N 42
4.43. Contingência da biometria 42
4.44. Pessoa sem templates 42
4.45. Pessoa com template inválido 43
4.46. Obtenção da biometria 43
4.47. Uso do display 43
4.48. Utilização de urna / cofre coletor 44
4.49. Digitação de função 44
4.50. Início e fim da validação 44
4.51. Criptografia de crachás 45
4.52. Gravação do Smart Card 45
4.53. Timeout de validação na DFS 45
4.54. Tempo de validação Off-line 45
4.55. Margem de erro da revista aleatória 45
5. Eventos 47
5.1. Monitoramento das entradas digitais 47
5.2. Entradas digitais dependentes 47
5.3. Dispositivo alarmado 47
5.4. Evento mascarado 47
5.5. Burla de catraca 48
5.6. Desistência de acesso 48
5.7. Evento de acesso 48
5.8. Direção do acesso 48
5.9. Dispositivo fora do estado de repouso 49
5.10. Intrusão 49
5.11. Envio do evento 49

5.12. Persistência dos eventos 49
5.13. Eventos com informações cadastradas 50
5.14. Capacidade de armazenamento de eventos 50
5.15. Limite de eventos enviados 50
6. Biometrias 51
6.1. Cadastro de digitais Sagem 51
6.2. Capacidade suporte para Sagem 51
6.3. Capacidade do sensor Suprema 51
6.4. Cadastro de biometria Suprema 52
6.5. Espaço reservado para validação de acesso 52
6.6. Cadastro de Handkey Recognition System 52
6.7. Restrições do cadastro de biometria 52
6.8. Ativação do cadastro 53
6.9. Cadastro da biometria 53
6.10. Gravação de SmartCard 53
6.11. Erro no cadastro 54
6.12. Fabricantes suportados 54
6.13. Templates já existentes 54
6.14. Validação de acesso 54
6.15. Armazenamento das templates 55
6.16. Atualização de biometria 55
6.17. Quantidade máxima de usuários/templates 55
7. Inicialização 56
7.1. Condição de inicialização 56
7.2. Opções de menu 56
7.3. Execução de teste 56
7.4. Configuração de rede 56
7.5. Atualização off-line 57
8. Acionamentos 58
8.1. Ativação de emergência 58
8.2. Ativação de emergência com crachá mestre 58
8.3. Acionamentos possíveis 58
8.4. Acionamentos programados 59
8.5. Acionamentos por eventos 59
8.6. Tempo de acionamento 59
8.7. Entradas digitais 60
8.8. Restrições de acionamentos 60
8.9. Acionamentos de revista aleatória 60

8.10. Mascaramento de entradas digitais..... 60
9. Problemas, compreendendo e resolvendo 62
10. Histórico de revisões do manual 62
11. Glossário 63

1. Objetivos

Os objetivos deste documento são descrever de forma direta os 182 (cento e oitenta e dois) requisitos funcionais e não funcionais da solução firmware e middleware Digicon para Acesso com as controladoras MCA (Power PC) e MCANet (Arm-9).

Para melhor entendimento e aplicação de uso, os requisitos foram agrupados em 7 (sete) casos:

1. Comandos;
2. Configurações;
3. Validações;
4. Eventos;
5. Biometrias;
6. Inicialização e
7. Acionamentos.

É reservado a Digicon o direito de qualquer alteração sem consulta prévia.

2. Comandos

A execução de comandos no firmware do dispositivo possibilita o controle do dispositivo pelo sistema. Envio ou captura de informações ou configurações do dispositivo podem ser executados a partir de comandos. Como exemplo, um comando para captura de marcações (backup).

Embora o caso de uso tenha interação com pessoas, essa interação é feita através dos dispositivos Digicon. Assim a interface utilizada é o próprio dispositivo, não cabendo o desenho de protótipos.

2.1. Carga de lista de permissão de faixa horária

Deve ser possível carregar lista de permissão indicando as faixas horárias da permissão.

- Para cada permissão deve indicar as faixas horárias em que o acesso é liberado. Caso não seja informado as faixas horárias devem gerar um retorno de erro na execução do comando.

- Deve indicar quais as leitoras da permissão. Se não existir a indicação das leitoras deve gerar um retorno de erro na execução do comando.

2.2. Lista de feriados

Deve permitir carregar uma lista contendo os feriados que o firmware deve levar em consideração ao realizar uma validação de acesso.

- A lista deve conter a data do feriado, com as informações de dia, mês e ano. Caso não tenha uma das informações a lista de feriados deve ser descartada, deve ser gerado um retorno de erro na execução do comando e registrado o erro no log do firmware.

- Caso a lista de feriado contenha a mesma data mais de uma vez, deve considerar apenas uma data, desprezando as outras datas iguais.

2.3. Lista de liberação

Deve ser possível informar uma lista contendo os crachás que tem permissão de acesso no dispositivo.

- Deve indicar um identificador único de acesso (crachá, identificador de pessoa, etc...).

- Deve indicar em quais leitoras a pessoa tem acesso permitido e em quais leitoras a pessoa tem acesso negado.

- Caso não tenha qualquer uma das informações, deve gerar um retorno de erro na execução do comando, gravar um log informando o erro e rejeitar toda a lista.

2.4. Lista de templates biométricos

Deve ser possível carregar uma lista de templates biométricos no dispositivo.

- Deve indicar em quais leitoras de biometria a lista deve ser carregada. Caso não seja indicado deve recusar o comando gerando retorno de erro e gravando log informando que não foi informada a leitora biométrica.

- Deve indicar a pessoa e as suas templates. Caso a pessoa não seja indicada deve gerar retorno de comando com erro indicando que falta a identificação da pessoa.

- Caso a pessoa não tenha templates deve gerar um retorno de erro na execução de comando informando a pessoa que não possuir templates e gerar log.

- Deve possuir a quantidade de templates indicadas pelo fabricante da leitora de biometria. Caso o comando possua mais ou menos templates do que a o fabricante suporta por pessoa, deve gerar um retorno de erro na execução do comando indicando a pessoa com as informações incorretas e gerar log de erro.

- Caso a lista possua mais usuários do que a capacidade configurada para o sensor biométrico, o firmware deve retornar o comando como erro na execução e informar em seu log que a lista é maior do que a capacidade do sensor.

2.5. Comando de carga de lista de cadastro de pessoas

Deve ser possível carregar uma lista com o cadastro da pessoa.

- A lista deve associar identificador de pessoa com número de cadastro da pessoa. Caso falte a informação da pessoa ou do cadastro da pessoa deve gerar retorno de erro na execução do comando e gravar log informando o erro.

- Não devem possuir o mesmo número de cadastro associado aos identificadores de pessoas diferentes. Caso um número de cadastro seja associado a mais de um identificador de pessoa, deve gerar um retorno de erro na execução do comando e gravar um log informando o erro.

2.6. Lista de faixa horária de refeitório

Deve ser possível indicar as faixas horárias de uso do refeitório.

- Deve indicar os conjuntos de faixas horárias de acesso permitido ao refeitório.

- Deve indicar as leitoras onde o acesso é permitido.

- Caso não tenha qualquer uma das informações, deve gerar um retorno de erro na execução do comando e gravar log informando o erro.

2.7. Exclusão de lista

Deve ser possível excluir qualquer uma das listas mantidas pelo firmware.

- Deve indicar qual das listas deve ser excluída.

- Caso não tenha a indicação da lista que deve ser excluída o firmware deve retornar erro na execução do comando.

2.8. Status de lista

Deve retornar as informações sobre as listas do firmware.

- Deve indicar de qual lista deve retornar as informações.
- Deve retornar a quantidade de registros da lista.
- Deve retornar a data de última atualização da lista.
- Caso o comando não indique de qual lista é para retornar o status, deve gerar um retorno de erro na execução do comando informando que não foi definida a lista.
- Se a lista solicitada não existir o ou não existir nenhuma lista no firmware deve retornar como lista inexistente.

2.9. Mensagem do display

Durante a execução dos comandos de carga de lista o firmware deve escrever no display a mensagem “Bloqueado” na primeira linha e “Carga de lista” na segunda linha sempre que:

- Qualquer leitora ou leitor fique bloqueado pela execução do comando.
- O dispositivo possui display.

2.10. Inclusão de usuário biométrico (templates)

Deve ser possível incluir um conjunto de templates na lista de templates do firmware. Ao fazer esta inclusão o firmware deve carregar os templates na memória da leitora. Deve indicar em quais leitoras os templates deve ser carregados. Caso a indicação seja zero (0), deve incluir em todas as leitoras biométricas que o dispositivo possui.

- Caso não exista lista de templates, deve criar a lista neste momento.
- Caso o crachá já exista na lista, deve excluir os templates do crachá e então fazer a nova inclusão.
- Caso não tenha mais espaço na leitora biométrica para os templates, deve excluir os templates do crachá que está a mais tempo sem ser utilizado e incluir o novo.

2.11. Exclusão de usuário biométrico (templates)

Deve ser possível excluir os templates de um crachá da lista de templates do dispositivo e de suas leitoras biométricas. Deve indicar em quais leitoras os templates deve ser excluídos. Caso a indicação seja zero (0), deve excluir em todas as leitoras biométricas que o dispositivo tem.

- Deve excluir todos os templates associados ao crachá.

- Caso o crachá não exista na lista deve responder como comando executado com sucesso.

- Caso não exista a lista, deve responder como comando executado com sucesso.

2.12. Atualização de firmware

Deve possuir um comando para atualização do próprio firmware.

- Antes de iniciar a atualização o firmware deve encerrar todos os processos de validação de acesso, envio de eventos e execução de comandos.

- Ao iniciar a atualização o dispositivo deve ser bloqueado, escrevendo a mensagem "Atualizando Firmware" no display, caso o dispositivo tenha display.

- O firmware deve converter todos os arquivos de controle para a versão do firmware para a qual está sendo atualizado.

- O firmware deve guardar uma versão do firmware atual como backup durante a atualização. Caso ocorra falha na atualização o firmware deve reiniciar o dispositivo carregando o firmware backup.

- Ao encerrar a atualização do firmware o dispositivo deve ser desbloqueado, exibindo no display a mensagem default configurada, caso o dispositivo possua display.

- Caso não consiga converter o ID do dispositivo, deve setar o ID para zero.

2.13. Atualização para versão mais antiga

Caso a versão do firmware do comando de atualização seja menor que a versão do firmware atual do dispositivo, deve ser gerado um evento de controle indicando uma atualização para uma versão mais antiga do firmware e não deve ser feita a conversão dos arquivos do firmware.

2.14. Evento de atualização

Deve gerar um evento de controle de firmware atualizado, indicando a versão para o qual foi feita a atualização.

2.15. Comando de backup

O firmware deve possuir um recurso para recuperar os eventos de acesso já enviados, conforme as seguintes condições:

- Durante a recuperação o dispositivo deve ser bloqueado e exibir a mensagem: "Bloqueado Backup Eventos".

- Deve ser possível selecionar os eventos ocorridos durante o período informado e enviar estes eventos para o DFS.

- Deve receber como parâmetro o período em que deve efetuar a recuperação.

- Caso não seja informada a data inicial do período, deve considerar todos os eventos ocorridos até a data final.

- Caso não seja informada a data final do período, deve considerar todos os eventos ocorridos a partir da data inicial.

- Caso não seja informada nem a data inicial e nem a data final, deve considerar todos os eventos.

- Após a recuperação dos eventos deve desbloquear o dispositivo.

- No retorno do comando deve ser enviada a quantidade de eventos recuperados.

2.16. Configuração do dispositivo

Deve ser possível atualizar as informações de configuração e de propriedades do dispositivo através de comando.

- Deve ser possível alterar as configurações sem que seja necessário reiniciar o firmware manualmente.

- Deve ser possível alterar as configurações de endereçamento do firmware.

- Deve ser possível alterar as configurações de validação de acesso que o firmware realiza.

- Deve ser possível alterar as configurações de leitoras, entradas e saídas digitais do firmware.

- Deve ser possível alterar as configurações de horário de verão e UTC do firmware.

2.17. Atualização de data e hora

Deve ser possível atualizar a data e hora do dispositivo através de comando.

- Deve atualizar o RTC do sistema operacional do dispositivo.

2.18. Comando de status

Deve existir um comando que retorne as informações das configurações do dispositivo. Deve retornar as seguintes informações:

- Versão do firmware.

- Data e hora da última atualização do firmware,

- Data e hora da última atualização da configuração do firmware.
- Período do horário de verão.
- Data e hora atual do firmware.
- Status de bloqueio das leitoras.
- Status de ativação de estado de emergência do dispositivo.
- UTC do dispositivo.
- Configuração de rede do dispositivo - ID e IP.

2.19. Comando de bloqueio e desbloqueio de dispositivo

Deve ser possível bloquear e desbloquear o dispositivo através de comando.

- Deve informar quais as leitoras que devem ser bloqueadas ou desbloqueadas. Caso no comando não venha as informações da leitora, deve retornar o comando como erro na execução e registrar o erro em log.
- O estado das leitoras deve ser mantido ao iniciar o firmware, ou seja, as leitoras que estão com status de bloqueadas devem permanecer bloqueadas e as que estão desbloqueadas devem permanecer desbloqueadas.

2.20. Limpar arquivos de eventos

Deve ser possível limpar os arquivos de eventos de acesso e eventos de alarme enviados.

- Deve ser possível limpar somente os eventos de acesso, somente os de alarme ou ambos.
- Deve excluir somente os eventos que já tem confirmação de entrega.
- Caso não tenha nenhum evento para ser excluído deve indicar no log que o arquivo está vazio.

2.21. Ativar e desativar emergência

Deve ser possível ativar e desativar o estado de emergência do dispositivo.

- O estado de emergência deve desativar a validação de acesso do dispositivo, permitindo que todas as pessoas passem. Nas catracas e torniquetes, por exemplo, deve deixar o giro livre.
- Caso o firmware seja desligado em estado de emergência acionado, ao ser ligado deve retornar o estado de emergência acionado.

- Enquanto o estado de emergência estiver acionado o firmware deve exibir no display do dispositivo a mensagem "EMERGENCIA". Caso o dispositivo não possua display o firmware não deve exibir nenhuma mensagem.

2.22. Ativar e desativar monitoramento de alarmes

Deve permitir ativar o monitoramento das entradas digitais, gerando alarme para as mudanças de estado.

- Caso o monitoramento de alarmes esteja ativo, sempre que uma entrada digital mudar o seu estado o firmware deve gerar um alarme indicando a mudança.

- O estado de uma entrada digital pode ser acionado ou desligado.

2.23. Horário de verão

Deve ser possível indicar o período de horário de verão para o dispositivo.

- O período do horário de verão deve ter uma data inicial e uma data final. Caso uma das datas não seja informada o firmware deve gerar um retorno de erro indicando a falta da informação.

- O firmware deve considerar como horário de verão, desde as 00:00 (zero hora) da data inicial até as 23:59 da data final.

2.24. Ativar e desativar saída digital

Deve ser possível ativar e desativar uma saída digital do dispositivo.

- A saída digital deve estar configurada. Caso receba um comando de acionamento de saída digital sem que a saída esteja configurada o firmware deve gerar um retorno de erro na execução do comando informando que a saída digital é desconhecida.

- Deve ser informado o tempo de acionamento da saída digital. A saída digital deve ser acionada pelo tempo definido no comando.

- Caso o tempo não seja informado deve acionar a saída digital até que receba um comando de desativar a saída digital ou até que o firmware seja iniciado.

- Para desativar uma saída digital basta informar uma saída configurada. Ao receber o comando o firmware deve desativar a saída digital correspondente. Caso seja informada uma saída digital não configurada o firmware deve gerar um retorno de erro na execução do comando informando que a saída digital não está configurada.

2.25. Status de saída e entradas digitais

Deve ser possível consultar o status das saídas e entradas digitais configuradas no firmware.

- O firmware deve responder para cada saída ou entrada configurada o status correspondente.

- O Status deve ser de ativada ou desativada.

- Deve ser selecionado se é para enviar o status das saídas ou das entradas. Caso não tenha esta informação no comando deve enviar o status das saídas e das entradas.

2.26. Mapa do Smart Card

Deve ser possível carregar o mapa do Smart Card no firmware.

- Caso o firmware não consiga ler o mapa do Smart Card deve gerar um retorno de erro na execução do comando informando que não conseguiu ler o mapa.

2.27. Copiar arquivo de log

Deve ser possível copiar o arquivo de logs do firmware.

- Deve retornar o tamanho do arquivo e o próprio arquivo.

- Caso não possua arquivo de log, deve retornar o tamanho como sendo zero (0).

- Caso não consiga copiar o arquivo de log deve gerar retorno de erro na execução do comando informando que o arquivo de log do firmware apresenta problema.

2.28. Processos automáticos

Deve ser possível incluir processos para executar acionamentos de forma automática e agendada.

- Deve ser informada a saída digital que o processo deve acionar e a duração do acionamento e a data de início de execução. Caso a data de início de execução não seja informada deve gerar um retorno de erro na execução do comando informando que não foi enviada a data de início do acionamento.

- Deve ser informada a periodicidade do acionamento, ou seja, de quanto em quanto tempo deve o acionamento deve ser agendado. Caso não seja informado será executado apenas uma vez.

- Deve ser informada a quantidade de vezes que a saída digital deve ser acionada. Caso não seja informado será sempre agendada uma nova execução.

- Deve ser possível excluir os acionamentos agendados.

- Deve ser possível consultar os acionamentos agendados, com as informações da saída que será acionada e da data de próxima execução.

2.29. Comando não reconhecido

Ao receber um comando não reconhecido o firmware deve responder com erro na execução por comando não implementado.

2.30. Consistência das informações

Caso o firmware não consiga executar o comando com as informações recebidas, deve gerar um retorno de falha na execução informando que as informações do comando estão inconsistentes.

2.31. Log das informações

O firmware deve registrar a execução de cada comando indicando:

- Início e final da execução.
- Falhas de execução.

2.32. Tamanho das listas

O tamanho das listas enviadas nos comandos não deve ser maior que 600Kb. Este é o valor limite que o firmware pode receber e manter seu funcionamento, porém existem exceções que estão descritas a seguir:

- Para envio da lista de templates, o tamanho não deve ser maior que 2MB. Este valor é o limite que o firmware suporta.
- Para listas de cadastros de pessoas o tamanho deve ser limitado pela quantidade de registros, sendo a capacidade máxima de 15.000 registros.

Caso seja enviada uma lista maior que o limite, o firmware deve gerar um retorno de erro na execução do comando por limite de tamanho de lista. Além do retorno de erro deve logar o erro ocorrido na execução do comando.

2.33. Timeout de comandos

Caso o comando não seja recebido dentro do tempo de timeout pelo firmware o mesmo deve gerar um retorno de comando indicando erro na execução do comando por timeout. Deve também logar o erro ocorrido.

Observação: No caso do erro de comunicação quem vai gerar o retorno com erro é o DFS, pois é ele que está gerenciando a execução do comando.

2.34. Execução do comando

Todo comando deve possuir um retorno, indicando se foi executado com sucesso ou se ocorreu falha na execução.

- Em caso de falha na execução do comando o retorno de comando deve informar qual a falha que ocorreu.

- Em caso de sucesso na execução o retorno de comando pode possuir informações particulares de cada comando.

2.35. Mensagem para aplicação das configurações

Sempre que o firmware aplicar as configurações no dispositivo, deve escrever no display a mensagem “Aplicando configurações”.

- Caso o dispositivo não possua display não deve escrever a mensagem.

Observação:

A configuração do dispositivo é aplicada quando o firmware é iniciado ou quando recebe um comando de carga de aplicativo. Em algumas situações a aplicação da configuração é tão rápida que o usuário não perceberá a mensagem.

3. Configurações

Permitir que o operador de segurança possa configurar informações básicas do firmware utilizando o teclado e display do mesmo. Configurações avançadas só estarão disponíveis no arquivo de configuração.

Este caso de uso tem iteração com o operador de segurança, porém esta iteração é feita através de telas da aplicação de alto nível e do próprio equipamento, sendo que o caso de uso não tem como alterar nenhum dos dois, motivo pelo qual não existe protótipo de interface.

3.1. Ativação do modo configuração

Deve ser possível ativar a configuração do dispositivo via teclado.

- O dispositivo deve possuir teclado e display para que seja possível configurar manualmente.

- O dispositivo não deve permitir a configuração quanto estiver em operação. A configuração somente deve ser habilitada durante o período de iniciação do dispositivo.

3.2. Informações configuradas

Deve permitir configurar as informações necessárias para que o dispositivo conecte-se com ao DFS:

- Id do dispositivo.
- Utilização de IP Fixo ou DHCP.
- IP do dispositivo, caso seja IP Fixo.
- Máscara de sub-rede.
- Gateway.
- Endereço IP do DFS.
- Porta de comunicação do DFS.

3.3. Confirmação da configuração

O firmware deve solicitar confirmação da configuração ao usuário antes de assumir os novos valores da configuração.

- Caso o usuário não confirme as alterações o firmware deve cancelar a configuração e desprezar os valores digitados.

- Deve ser possível cancelar a configuração, desde que antes da confirmação.

3.4. Correções de informações digitadas

Deve ser possível corrigir informações digitadas.

- Após a confirmação da propriedade, somente deve ser possível cancelar toda a configuração.

3.5. Conferência das informações

O firmware deve verificar se os endereços IPs digitados na configuração manual têm a sintaxe válida:

- Caso um valor de endereço IP ou porta de comunicação não for válido o firmware deve cancelar a configuração, deixando em branco para o usuário poder informar novamente o endereço IP. Exemplo: ip 300.300.300.300 não é suportado.

- Caso seja digitada algum outro valor inválido ou maior que o suportado pela configuração o comportamento deve ser o mesmo. Indicar ao usuário que a configuração está incorreta, zerar o valor digitado e permitir digitar novamente a informação.

- Deve ser possível informar o IP zerado, 0.0.0.0. Nesse caso o firmware não irá alterar o IP configurado.

3.6. Identificação do dispositivo

O dispositivo deve possuir um identificador. A configuração manual deve possibilitar a alteração do identificador do dispositivo.

- Não deve permitir identificador zero ao configurar manualmente o dispositivo.

3.7. Bloqueio do teclado

Deve ser possível bloquear e desbloquear o teclado da MCA através do próprio teclado.

- O teclado deve ser sempre iniciado como desbloqueado.

- Dispositivos que não tem teclado sempre devem ser tratados como dispositivos com teclado bloqueado.

- Deve ser possível habilitar e desabilitar o recurso de bloqueio do teclado.

- Deve ser logado sempre que o teclado for bloqueado e sempre que o teclado for desbloqueado.

- Para bloquear o teclado deve-se teclar "entra" e em menos de 1 segundo teclar "Anula". Para desbloquear deve-se fazer o processo inverso, na mesma quantidade de tempo.

- Quando o teclado estiver bloqueado o evento não deve enviar nenhuma função digitada, enviando sempre a função padrão 0 (zero).

3.8. Configurações necessárias

Ao iniciar o firmware deve verificar se possui as configurações necessárias ao seu funcionamento.

- Caso não possua as configurações necessárias ou ocorra erro ao tentar configurar o dispositivo, o firmware deve bloquear as leitoras de crachá e biometria e escrever no display a mensagem "Bloqueado" caso o dispositivo possua display.

- Deve ler os valores default das entradas digitais, saídas digitais e solenóides. Para os valores que não o firmware não puder ler, deve assumir o valor zero (0) como default.

- Deve logar o sucesso e a falha na configuração do firmware.

3.9. Permissões do dispositivo

Ao iniciar o dispositivo deve carregar as permissões de acesso em que ele está inserido, juntamente com as faixas horárias de acesso de cada permissão.

- Caso o dispositivo não consiga carregar as permissões de acesso deve registrar em log que não carregou as permissões.

3.10. Mapa Smart Card

Caso o firmware possua leitoras de crachá Smart Card deve possuir as informações do mapa Smart Card.

- Se o firmware não conseguir carregar as informações do mapa Smart Card deve deixar as leitoras de crachá do tipo Smart Card desabilitadas e registrar em log que não conseguiu carregar o mapa Smart Card.

3.11. Exibir configurações

O firmware deve possibilitar a exibição de sua configuração. A exibição da configuração deve ser possível quando o firmware for executado por linha de comando.

3.12. Mensagem padrão

Caso o dispositivo possua display o firmware deve escrever no display a mensagem padrão de exibição configurada pelo usuário.

- O display do equipamento deve ficar em branco quando não existe mensagem padrão.

- Juntamente com a mensagem padrão o firmware deve exibir a informação de data e hora do dispositivo, a sinalização de capacidade e a sinalização de Status.

- Quando o firmware estiver funcionando em modo off-line deve exibir um símbolo de ponto (.) no canto inferior direito do display. Ao retornar ao funcionamento on-line o ponto deve ser removido.

3.13. Configurar propriedades

O firmware deve configurar as propriedades do dispositivo quando é iniciado. As propriedades que o firmware deve configurar são as mesmas propriedades persistidas no requisito Persistência das Propriedades.

- Caso não consiga setar alguma das propriedades persistidas o firmware deve logar qual a propriedade que não conseguiu configurar e bloquear o dispositivo.

3.14. Leitoras bloqueadas

Se ao iniciar o firmware verificar que todas as leitoras do dispositivo estão bloqueadas deve substituir a mensagem padrão pela mensagem “BLOQUEADO” no display do dispositivo.

- Assim que qualquer uma das leitoras do dispositivo for desbloqueada o firmware deve voltar a exibir a mensagem padrão configurado.

- Caso o dispositivo não possua display o firmware não deve exibir a mensagem.

3.15. Tratamento de conversões

O firmware deve verificar se as suas informações persistidas estão na mesma versão que a versão do firmware.

- Se as informações persistidas estiverem em versão mais antiga que a versão do firmware o firmware deve converter as informações persistidas para a versão do firmware. Se ocorrer erro na conversão o firmware deve logar o erro e bloquear o dispositivo.

- Se as informações persistidas estiverem em versão mais nova que a versão do firmware o firmware não deve alterar as informações persistidas. O firmware deve logar a diferença de versão e bloquear o dispositivo.

3.16. Conectar com Servidor

Ao ser iniciado e após carregar a sua configuração, conforme requisitos Configurações Necessárias, Permissões do Dispositivo, Mensagem Padrão, Configurar Propriedades o firmware deve aguardar um tempo aleatório dentro de um intervalo pré-definido e então conectar-se com a configurada. Caso a conexão falhe, o intervalo deve aumentar e o tempo deve ser novamente calculado e uma nova tentativa de conexão deve ser efetuada. Após três tentativas deve iniciar o ciclo novamente.

- Caso o firmware não tenha configurado o endereço ou a porta de comunicação do Servidor configurado não deve conectar-se com o Servidor.

- Na conexão o firmware deve identificar-se unicamente e enviar o endereço IP que está usando para a conexão.

- O firmware deve identificar a sua versão para o DFS na conexão.

3.17. Sincronismo de informações

Ao iniciar o firmware deve verificar se as suas informações estão sincronizadas com o DFS.

- Deve receber as alterações de biometria das pessoas.
- Deve receber as alterações de crachás de pessoas que utilizam a validação com biometria.
- Caso o firmware não possua nenhum templates armazenado não deve proceder a sincronização.
- Durante a execução do sincronismo deve exibir no display a mensagem "Sincronizando", caso o dispositivo possua display.

3.18. Desligar saídas, sensores e display

Quando o firmware for finalizado por ação do usuário o firmware deve:

- Limpar o display, caso o dispositivo possua.
- Retornar as saídas digitais e solenóides para o estado default configurado.
- Desligar urna e sensores biométricos.
- Desligar pictogramas.
- Desligar catraca deixando o acesso livre.
- O firmware somente deve desligar itens que o dispositivo possua e que esteja configurado, pois nos demais casos o firmware não tem controle sobre o equipamento.

3.19. Persistência das propriedades

O firmware deve persistir todas as informações de propriedades necessárias ao seu funcionamento, conforme Informações Configuradas.

- O firmware deve persistir também os valores default configurados para as entradas digitais, saídas digitais e solenóides, conforme Valores Default.

3.20. Mensagem por evento

Cada tipo de evento de acesso deve possuir uma mensagem padrão para exibição no display.

- Na ocorrência do evento de acesso o firmware deve exibir a mensagem corresponde do evento.
- Deve ser possível configurar mensagem diferente da mensagem padrão para cada tipo de evento. Quanto existir mensagem configurada para o tipo de evento deve exibir a mensagem configurada ao invés da mensagem padrão.

- A mensagem deve ter tamanho compatível com a capacidade do display do dispositivo. Caso a mensagem seja maior que a capacidade do display o firmware deve exibir somente a quantidade que cabe no display desprezando o resto da mensagem. Exemplo: Se a mensagem for "Acesso Negado - Passe no RH para conferência da Carteira de trabalho" e o display for de 32 dígitos, deve exibir "Acesso Negado - Passe no RH para".

3.21. Exibição de data e hora

Deve ser possível configurar o dispositivo de modo que ao exibir mensagens que contenham data e hora a data e hora sejam sempre em relação ao configurado para o dispositivo, mesmo que em UTC diferente da aplicação ou UTC diferente do Middleware.

- A exibição da data e hora sempre será em relação ao próprio dispositivo.

3.22. Horário de verão

Deve ser possível configurar período de horário de verão para o dispositivo.

- Em caso de ter horário de verão configurado o firmware deve exibir data e hora com base no UTC e horário de verão configurado.

3.23. Acionamentos de emergência

Deve ser possível configurar os seguintes acionamentos para execução quando o dispositivo entrar em estado de emergência.

- Saída digital.
- Solenóide.
- Pictograma.
- Display - Com a mensagem para escrever.
- Urna.
- Buzzer.

Deve ser possível configurar para que o acionamento ocorra durante um tempo determinado ou que ocorra durante todo o tempo em que o dispositivo esteja em estado de emergência.

3.24. Funções

Em dispositivos que possuem teclado e display deve ser possível configurar funções para uso do teclado.

- A função deve ser relacionada com uma tecla numérica do teclado.

- A mesma função não pode ser relacionada a duas teclas diferentes.

- A função deve ter um tempo de acionamento, sendo que após decorrer o tempo o firmware deve cancelar o uso da função caso o firmware não tenha detectado nenhuma ação - Passagem de crachá ou digitação no teclado.

- A função pode ter mensagem de ativação e de finalização. Caso não tenha mensagem de ativação configuração, ao ser ativada deve escrever no display a mensagem "Função X --> YY", onde X é a tecla pressionada para ativar a função e YY é a contagem regressiva de tempo para a função ser desativada.

3.25. Tamanho de arquivos

Deve ser possível configurar o tamanho dos arquivos do firmware para cada tipo de arquivo.

- O tamanho padrão dos arquivos de eventos e alarmes é de 256 kb. O tamanho mínimo é de 10kb.

- O tamanho do arquivo de logs é de 64 Kb e o tamanho mínimo é de 10 Kb.

- O firmware não deve permitir mudar o tamanho dos arquivos para menor que o tamanho mínino. Neste caso deve gerar erro e logar a tentativa de reduzir o arquivo para menos que o tamanho mínimo.

- O firmware não deve aceitar diminuir o tamanho dos arquivos de eventos não enviados se estes arquivos estiverem com eventos gravados.

3.26. Valores default

Deve ser possível configurar os valores de estado default para:

- Todas as entradas digitais do dispositivo.

- Todas as saídas digitais do dispositivo.

- Todas as solenóides do dispositivo.

Os valores default possíveis são zero (0) e um (1).

3.27. Duplicação de templates biométricos

Observação:

O sensor biométrico SAGEM possui configuração para habilitar o cadastro de templates biométricos duplicados. Com essa opção habilitada, ou seja, aceitando templates duplicados, o sensor SAGEM não faz a consistência das biometrias, inserindo-as de maneira mais rápida (média de 400 milissegundos). Uma conseqüência desta opção é que quando houver templates duplicados no sensor, com a validação 1:N habilitada, o sensor sempre vai devolver a primeira template localizada.

Por padrão, essa definição será sempre por aceitar templates duplicados.

Essa configuração deve ser exclusiva para leitoras do fabricante SAGEM.

3.28. Controle SAD

Deve ser possível configurar para cada leitor do dispositivos se utiliza o controle SAD.

Quando utilizar este controle, o dispositivo deve armazenar qual é o número do seu SAD, conforme Tamanho de arquivos.

3.29. Leitora

Deve ser possível configurar para cada leitora do dispositivo quais as validações de acesso que realiza, conforme Validar Acesso.

- Caso seja configurada uma leitora que o dispositivo não possua o dispositivo deve recusar a configuração gerando um retorno de erro no comando de configuração e logar o erro ocorrido.

3.30. Acionamentos da validação de acesso

Deve ser possível configurar acionamentos para o resultado da validação de acesso, com resultado de acesso permitido ou acesso negado. Deve ser possível configurar acionamentos de:

- Saída digital.
- Solenóide.
- Pictograma.
- Display - Com a mensagem para escrever.
- Urna.
- Buzzer.

Para cada acionamento deve ser possível informar o tempo de acionamento e o estado inicial.

3.31. RFID

Deve ser possível configurar a formatação do número de crachá.

- A configuração deve indicar o tipo de leitora RFID e o protocolo que deve ser utilizado.

- A configuração deve indicar também se lê apenas o número do crachá ou o número do crachá junto com o facility code.

- O valor default de leitura é somente ler o número físico.

3.32. Barras

Deve ser possível configurar a formatação do número de crachá de barras.

- A configuração deve indicar o tipo de criptografia. Quando não indicar o tipo de criptografia deve assumir que o tipo é sem criptografia.

- Quando não utilizar criptografia pode-se indicar descartes de dígitos conforme a máscara do crachá.

3.33. SmartCard como proximidade

O firmware deve permitir o uso de crachás de tecnologia SmartCard como proximidade.

Nesse caso o firmware deve ler o numero físico do crachá SmartCard e fazer a validação de acesso conforme o requisito:

On-line / Off-line.

3.34. Acionamentos de alarme

Deve ser possível configurar acionamentos para quando uma entrada digital for alarmada. Para uma entrada digital ser considerada alarmada ela deve estar configurado com:

- Estado padrão - Quando a entrada digital está neste estado não é considerada alarmada. Quando o estado da entrada digital for diferente do estado padrão a entrada é considerada alarmada.

- Leitora associada - Caso exista uma leitora associada à entrada digital o sinal não deve ser considerado. Neste caso deve possuir um tempo de acionamento, sendo que se a entrada for acionada por mais tempo que o tempo configurado a entrada deve ser considerada alarmada.

A configuração do acionamento entrada digital deve possuir:

- Acionamento, podendo ser:

- Saída digital.

- Solenóide.

- Pictograma.

- Display.

- Buzzer.

- Tempo de acionamento - Pode ser configurado um tempo de acionamento. Caso não seja configurado o acionamento será durante todo o tempo em que a entrada digital estiver acionada.

- Período de mascaramento - Pode ser informado um período durante o qual um sinal na entrada digital não transforma o status em entrada alarmada. O período deve ter obrigatoriamente um início e um fim.

- Geração de evento - Pode ser configurado para que uma entrada digital gere evento de alarme quando estiver alarmada. Mesmo que a entrada esteja em período de mascaramento o evento de alarme deve ser gerado.

- Tempo de delay (espera) - Pode ser configurado um tempo em que a mudança do estado da entrada digital não será considerada como alarmada. Somente após este tempo a entrada será considerada alarmada.

- Uso do display - A entrada digital pode ser configurada para que caso entre em estado de alarmada sinalize no display que está alarmada. Caso o dispositivo não possua display, não deve utilizar esta configuração.

3.35. Configurar por linha de comando

Deve ser possível configurar o endereçamento do dispositivo e do DFS via linha de comando do sistema operacional.

- Para assumir a nova configuração o firmware deve ser iniciado.

- Antes de assumir a nova configuração o firmware deve validar o endereçamento IP.

- O firmware deve exibir a configuração atual e solicitar ao usuário se deseja alterar a configuração.

- Caso a configuração por linha de comando seja interrompida, o firmware deve assumir a última configuração válida.

- O firmware deve solicitar confirmação do usuário antes de assumir a nova configuração.

- As informações que o firmware deve solicitar são as mesmas da configuração manual pelo teclado.

- Caso seja deixado o campo em branco, deve assumir o valor anterior para a informação.

3.36. Utilização de DHCP

Quando o dispositivo utilizar endereçamento via DHCP não deve ser necessário guardar o seu endereço IP, porém não é obrigatório que o IP seja alterado toda vez que o dispositivo for iniciado.

3.37. IP Fixo

Caso o dispositivo utilize IP fixo este IP deve ser armazenado e mesmo quando for iniciado deve manter o mesmo endereço IP.

- No caso de utilização de IP fixo o endereço IP somente poderá ser alterado por uma das formas de configuração.

- Se o dispositivo trabalhar com IP fixo e não possuir IP configurado Não deve ser possível conectar com o DFS.

3.38. Timeout de execução de comandos

Deve ser possível configurar o tempo de timeout de execução dos comandos.

- O tempo de timeout deve ser o mesmo para todos os comandos com exceção dos comandos de carga de lista.
- Caso o timeout não seja configurado deve utilizar o tempo de 6 segundos.
- Para os comandos de carga de lista o tempo de timeout deve ser calculado conforme o tamanho da lista.

3.39. Timeout do envio de eventos e requisições de acesso

Deve ser possível configurar o tempo de timeout em segundos do envio de eventos e requisições de acesso. O timeout é o tempo máximo que o firmware deve esperar a confirmação do envio de um evento e de um retorno de uma requisição de acesso.

- O tempo do timeout deve ser o mesmo para eventos e requisições de acesso.
- Caso o timeout não seja configurado deve utilizar o tempo de 3 segundos.
- Caso o timeout seja menor do que 3 segundos, assumir 3 segundos.
- Caso o timeout seja maior do que 20 segundos, assumir 20 segundos.
- Caso o Servidor não responda até o tempo máximo configurado, o firmware deve assumir que está off-line. O evento de acesso deve ser reenviado e a requisição deve continuar de maneira off-line de acordo com a tecnologia do crachá.

3.40. Configurações de leitoras

Ao configurar as leitoras do dispositivo caso ocorra algum erro o firmware deve para a configuração da leitora que apresentou problemas e continuar na próxima.

- Ao final da configuração de todas as leitoras do dispositivo o firmware deve apresentar uma mensagem no log informando quais foram configuradas corretamente e quais apresentaram erro.

3.41. Configuração da revista

Deve ser possível configurar para que o firmware execute a funcionalidade de revista aleatória.

- Deve ser definido entre 1 e 7 faixas horárias para que a revista seja executada. Caso não seja informado nenhum horário de revista o firmware deve recusar a

configuração enviando um retorno de erro no comando que enviou a configuração.

- A configuração da revista aleatória deve ser feita por leitor.

3.42. Tipos de crachá

Deve ser possível informar os tipos de crachás que farão parte da revista e o percentual de probabilidade do tipo ser sorteado, por exemplo: Empregado: 20%; Visitante: 5%.

- Tipos de crachá não informados ou com percentual igual a 0% não devem participar do sorteio.

Observação: O sorteio deve ser programado tendo como base a probabilidade de sorteio por tipo de pessoa, porém, não tem obrigação de ser exato por dia. Ao longo do tempo, entretanto, deve aproximar-se do percentual estabelecido contando com a margem de erro.

Exemplo: Configurando o tipo Empregado para sortear 20%, se pegar os sorteados em um dia pode resultar em 15% do total de empregados em um dispositivo, porém, a média de uma semana em todos os dispositivos deve ser de 20% com margem de erro de 10%. Maiores informações, vide requisito de quantidade de sorteados.

3.43. Acionamentos da revista

Deve ser possível configurar acionamentos para execução na revista aleatória, porém não é obrigatório ter algum acionamento configurado.

- Deve ser possível configurar os mesmo tipos de acionamentos da validação de acesso.

- No caso de existir algum acionamento do display com exibição de mensagem, a mensagem da revista aleatória deve sobrepor as demais mensagens como a mensagem do retorno da validação de acesso e mensagens cadastradas para o colaborador.

3.44. Restrições da configuração

O firmware não deve permitir as seguintes configurações em conjunto com a revista aleatória:

- Controle de crédito de acesso.

- Validação de autorizador.

Caso o firmware receba o comando de configuração com estas validações em conjunto, deve recusar o comando informando que não pode realizar a revista aleatória com as outras validações.

3.45. Validação de autenticidade do BDCC por tipo de crachá

Deve ser possível informar os tipos de crachás que farão a validação de autenticidade do BDCC.

- A configuração deve ser por leitora.

Ex: pode-se validar o crachá de empregado como BDCC e o de visitante de modo normal, sem autenticação BDCC.

4. Validações

Validar o Acesso do usuário do crachá, podendo ser no próprio cartão (SmartCard), no dispositivo, no Middleware e no sistema.

A validação do acesso é realizada a partir da leitura do cartão.

4.1. Validação de crachás do BDCC

O firmware deve permitir a verificação de autenticidade de crachás gravados pelo BDCC.

Caso a verificação de autenticidade não esteja habilitada, o firmware deve fazer a validação do crachá SmartCard sem a verificação de autenticidade.

A verificação de autenticidade deve ocorrer da seguinte maneira:

Leitura dos dados gravados no crachá.
Descriptografar os dados.
Comparar o ID gravado criptografado no crachá com o ID real do crachá (fabricante).

4.2. Leitura dos dados gravados no crachá

Para leitura dos dados gravados no crachá, o firmware deve verificar o mapa smart card específico do BDCC. Este mapa deve possuir a localização dos dados criptografados gravados pelo BDCC.

4.3. Descriptografia dos dados de crachás do BDCC

O firmware deve descriptografar os dados lidos de crachás do BDCC. Para descriptografar os dados, o firmware deve utilizar a chave previamente carregada no dispositivo. Caso essa chave não exista, deve ser gerado um evento de alarme informando que o firmware não possui a chave para descriptografia do crachá e o acesso deve ser negado.

A criptografia utilizada e a forma de leitura do crachá smart card está definido no item II. Dados Criptografados do documento "EspecificaçãoTécnicaBDCC_AnexoIV_V1-0.pdf".

4.4. Comparação de ID descriptografado com ID real

Após a descriptografia das informações contidas no crachá smart card, o firmware deve comparar o identificador obtido com o identificador real do crachá. Caso os identificadores não sejam iguais, o firmware deve:

- Gerar um evento de acesso para o crachá informando que o acesso foi bloqueado pela validação do BDCC.

- Exibir a uma mensagem no display conforme configuração, informando que o crachá não foi autorizado.

- **Bloquear o acesso**.

4.5. Ausência de campo no mapa do Smart Card

Caso a atualização do crachá não seja feita pela falta da informação no mapa do Smart Card o firmware deve gerar um evento de alarme indicando que existe atualização de informação que não está no mapa do cartão.

- Não deve gerar o evento de crachá atualizado.

4.6. Atualização de pendências

A atualização de pendências deve ocorrer quando o retorno da validação de acesso no DFS enviar pendências para atualização no crachá e a tecnologia configurada pra o crachá é SmartCard.

- Caso o firmware consiga gravar as atualizações no crachá deve gerar um evento de alarme de crachá atualizado, informando a data e hora da atualização.

Deve atualizar a data de última atualização do crachá, no crachá, ao gravar as pendências no SmartCard.

4.7. Permissão

Validar permissões de acesso de acordo com os requisitos do Validar Acesso:

- Permissão da pessoa ou crachá.

- Faixa horária da permissão.

- Permissões adicionais.

Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.8. Situação

Verificar a situação da pessoa ou crachá conforme requisitos do Validar Acesso:

- Situação do crachá.

- Bloqueio por faltas

- Validade do crachá

Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.9. Afastamento

Deve validar se existe afastamento para o crachá conforme Validar Acesso:

- Verificar afastamento.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.10. Crédito de acesso

Validar crédito de acesso conforme requisito Validar Acesso:

- Crédito de acesso.
- Controle da faixa de consumo de crédito.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.11. Faixa horária do crachá

Deve validar a faixa horária do crachá conforme Validar Acesso:

- Faixas horárias.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.12. Crachá mestre

Deve tratar crachá mestre conforme Validar Acesso:

- Controle de crachá mestre.

4.13. Exibição de mensagem

Deve exibir mensagem para a pessoa conforme Validar Acesso:

- Exibição de mensagem.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.14. Senha

Deve realizar a validação com senha conforme Validar Acesso:

- Validação com senha.

- Deve utilizar as informações do crachá ao invés das informações da pessoa.

- Caso o DFS retorne a senha da pessoa na validação de acesso o firmware deve verificar se a pessoa e o dispositivo validam senha.

- Deve ser possível configurar o dispositivo para pedir sempre a senha, nunca pedir senha ou pedir senha de acordo com a pessoa.

- Se ambos validam senha ou se o dispositivo sempre valida senha, o firmware deve solicitar a senha da pessoa. Após a digitação da senha o firmware deve comparar a senha da pessoa com a senha digitada. Se forem iguais o acesso deve ser liberado. Se forem diferente o acesso deve ser negado.

- Caso o firmware peça a senha e a pessoa não informe toda a senha em 10 segundos, o firmware deve considerar como senha inválida e negar o acesso da pessoa.

4.15. Intervalo mínimo de almoço

Deve realizar a validação com senha conforme Validar Acesso:

- Controle de intervalo mínimo de almoço.

Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.16. Interjornada

Deve realizar a validação com senha conforme Validar Acesso:

- Controle de interjornada.

- Tempo de interjornada.

- Configuração dos tempos.

- Data de saída.

- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.17. Autorização de entrada

Crachás do tipo autorização de entrada devem validar na pessoa somente os seguintes itens:

- Situação do crachá.

- Validade do crachá.

- Nível.

- Anti-dupla.
- Permissão de acesso.
- Biometria.

4.18. Controle de Nível

Deve controlar nível e anti-dupla conforme o Validar Acesso:

- Controle de nível.
- Exceções do nível.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.19. Validade do crachá

Deve verificar se o crachá está dentro da validade, ou seja, se a data e hora do acesso é menor ou igual a data e hora final da validade do crachá.

- Caso não possua a hora final de validade do crachá, deve considerar 23:59.
- Caso a data do final da validade do crachá seja em branco deve considerar como inexistente e neste caso permitir o acesso.

4.20. Controle de Anti-dupla

Deve controlar nível e anti-dupla conforme o Validar Acesso:

- Controle de anti-dupla.
- Anti-dupla temporizado.
- Deve utilizar as informações do crachá ao invés das informações da pessoa.

4.21. Crachá com chave padrão

Sempre que o firmware detectar que o crachá apresentado na leitora smart card está com a chave padrão de fábrica o firmware deve gravar a chave do mapa smart card no lugar da chave padrão e em seguida atualizar todas as informações do cartão.

4.22. Crachá desatualizado

Caso o firmware esteja off-line durante a validação de acesso o mesmo deve verificar se o crachá está desatualizado. Caso esteja o firmware deve negar o acesso gerando o evento de "Acesso negado por crachá desatualizado".

- Exemplo de crachá desatualizado: Data atual: 05/05/2011. Data da última atualização do crachá: 01/04/2011. Tempo de expiração de pendência: 30 dias.

Neste caso a diferença entre as datas é de 35 dias (05/05/2011 - 01/04/2011) que é maior do que 30 dias, logo, o acesso será negado.

- A mensagem padrão para o acesso negado por crachá desatualizado é "Crachá desatualizado".

4.23. Atualizar somente crachás smart card

O firmware deve atualizar somente dados de crachás que foram configurados como smart card. Ou seja, um crachá smart card que foi configurado como proximidade não deve ter as suas informações atualizadas.

4.24. Autorizador

Deve ser possível realizar a validação de acesso dependente de autorizador. Desta forma a pessoa deve ter o seu acesso válido além de necessitar da passagem de um crachá autorizador que também deve possuir acesso válido. Essa validação deve ocorrer de forma on-line, com comunicação até o Servidor.

- Deve ser possível configurar um tempo máximo de espera pela passagem do crachá do autorizador. Caso este tempo não seja informado deve utilizar como default o valor de 5 segundos.

- Quando necessitar de validação de autorizador, o autorizador deve passar o crachá dentro do tempo máximo configurado como timeout. Caso o autorizador não passe o crachá deve gerar um evento de "Acesso negado, Aguardando próxima validação".

- Caso mais de uma pessoa passe necessitando do mesmo autorizador, todas as validações devem permanecer pendentes da passagem do crachá de autorizador. Neste caso o tempo máximo de espera reinicia a cada passagem de crachá.

- Caso existam pessoas na fila esperando para serem autorizadas e um crachá que não é autorizador nem tem o mesmo autorizador dos demais é passado, deve ser gerado um evento de "acesso negado acompanhante" para cada crachá na fila.

- Deve ser possível configurar a quantidade máxima de pessoas escoltadas de uma só vez, sendo que o máximo para dispositivos sem catraca é de 255 pessoas e de dispositivos com catraca é de 1 pessoa.

- Sempre devem ser notificados os eventos de todos os crachás que estão na fila e do autorizador que autorizou o acesso.

- Caso ocorra uma desistência de acesso, essa desistência deve ser notificada apenas para o acompanhante.

- As validações do autorizador e autorizado devem ser feitas conforme Timeout de validação do servidor.

- Deve realizar a validação de biometria do autorizador e autorizado, quando configurado para tanto.

4.25. Revista aleatória

Deve ser possível executar a funcionalidade de revista aleatória no firmware, conforme o retorno da validação de acesso que deve indicar se a pessoa pode ou não participar da revista aleatória.

Caso o firmware esteja off-line com o DFS o firmware deve realizar o sorteio conforme sua configuração. Neste caso somente deve sortear pessoas dos tipos de pessoa configurados com percentual maior que zero (0%).

No caso da leitora controlar ambos os sentidos - Entrada e Saída - a revista aleatória deve ocorrer apenas na saída.

- Neste caso a leitora deve estar configurada para controlar nível.

4.26. Quantidade de pessoas sorteadas

Deve ser possível indicar percentualmente a quantidade de pessoas que devem ser sorteadas por dia de revista.

- O sorteio deve levar em consideração o percentual de revistados por dia como sendo a chance da pessoa ser revistada. Por exemplo, se for determinado o percentual de 20% das pessoas serem revistadas, a fórmula de cálculo para determinar se a pessoa que está validando o acesso deve gerar 20% de chance da pessoa ser sorteada e 80% de chance da pessoa não ser sorteada.

- Deve ser possível configurar percentual diferente para cada tipo de pessoa.

- Os tipos de pessoas não configurados ou configurados com percentual 0 (zero) não devem participar do sorteio de revista aleatório.

- Crachás do tipo mestre não devem ser sorteados, mas podem ser selecionados.

Observação: No firmware o percentual será utilizado como sendo a probabilidade da pessoa ser sorteada, pois o firmware não conhece o total de pessoal da maneira que o DFS conhece. O firmware também não sabe o total de pessoas já sorteadas.

4.27. Revistados de forma imperativa

Sempre que a requisição de acesso retornar que determinada pessoa seja revistada o firmware deve proceder como se a pessoa fosse sorteada para a revista, independente do tipo de pessoa estar configurado para ser revistado.

- Deve existir pelo menos um tipo de pessoa configurado para revista aleatória para que o firmware execute os procedimentos da revista.

- A indicação do retorno da validação de acesso é superior a qualquer outra indicação sobre revista aleatória.

- Quando estiver off-line a revista aleatória sempre será por sorteio.

Exemplo: O DFS retornou que o visitante XPTO deve ser revistado. Neste caso será como se o XPTO viesse do resultado do sorteio, e, mesmo que não tenho configurado para sortear visitantes, a pessoa XPTO deve ser revistada.

4.28. Acesso negado antes da revista aleatória

A pessoa somente poderá participar do sorteio de revista aleatória caso tiver o acesso permitido. O sorteio deverá ser efetuado após as demais validações, inclusive de biometria e senha.

Observações:

1 - Este requisito é necessário para impedir que um acesso negado seja transformado em acesso permitido. Por exemplo, uma pessoa tem o acesso negado pela faixa horária e é sorteada para a revista. Após ser revistada a pessoa pode sair, mesmo estando fora da faixa.

2 - Mesmo quando a pessoa está cadastrada na lista para ser revistada, o acesso da pessoa deve ser permitido.

3 - Após o acesso ser permitido o sorteio é feito e, se a pessoa for selecionada para a revista o evento de acesso poderá ser de acesso negado revista aleatória, dependendo da forma como está configurado.

4.29. Controle SAD

O sistema deve permitir o acesso de um crachá titular de empregado de uma mesma empresa porém, filiais diferentes, cadastrado ou não na base de dados, conforme diagrama FB0010.

Dispositivo On-Line: Quando o dispositivo estiver on-line com o DFS, a responsabilidade da validação do SAD será do DFS, conforme Validar Acesso – Controle SAD.

Dispositivo Off-Line: O crachá titular de empregado de SAD estrangeiro deve ter acesso permitido a base de dados se o mesmo não constar na lista de bloqueio ou se o dispositivo estiver operando com lista de liberação. A busca do crachá titular é realizada através do Máscara do Crachá e do Identificador de uso do crachá. **Importante:** Como o dispositivo não possui a relação do número físico para número lógico do crachá, quando o dispositivo estiver off-line este controle somente irá funcionar se o número lógico do crachá for igual ao número físico do crachá.

Observação importante: Para o controle do SAD é necessário que o leitor tenha esta opção configurada, conforme Configuração do firmware – Controle SAD.

4.30. Máscara do crachá

O dispositivo deve ser capaz de realizar a leitura da máscara do crachá quando estiver operando off-line.

4.31. Identificador de uso do crachá

O dispositivo deve ser capaz de obter o uso do crachá através do identificador de uso do crachá. Para isso, deve ser armazenada a lista “de para” do identificador de uso do crachá para o uso do crachá, conforme requisito Permissão.

Caso a máscara do crachá não possua a informação do identificador de uso do crachá, considerar o valor do identificador de uso do crachá como '0' e logar como warning.

4.32. On-line / Off-line

A validação de acesso deve ser feita no DFS quando o status do dispositivo for on-line. Quando o status do dispositivo for off-line, a validação de acesso deve ser feita no dispositivo.

Quando a tecnologia do crachá for Smart Card e o dispositivo não estiver fazendo a validação Smart Card como proximidade o firmware deve validar o crachá conforme os requisitos da validação Smart Card. Nos outros casos, a validação deve ser feita pelas listas.

4.33. Lista de liberação / bloqueio

Deve ser possível utilizar lista de liberação ou bloqueio para validar o acesso das pessoas.

- Quando o sistema estiver off-line e a validação não for de tecnologia Smart Card a validação obrigatoriamente deve ser feita com a lista de liberação. Se o crachá não estiver na lista de liberação o firmware deve negar o acesso, exibir no display a mensagem correspondente de acesso negado pela lista de liberação, gerar evento e logar a ocorrência.

- Deve ser possível utilizar a lista de liberação/bloqueio em todas as validações, mesmo on-line e com Smart Card.

4.34. Validação no DFS

Sempre que o firmware estiver on-line com o DFS a validação do acesso deve ser requisitada para o DFS.

- Caso o DFS demore mais de 2 (dois) segundos para responder a requisição de acesso o firmware deve efetuar a validação de acesso com as informações locais (Crachá Smart Card, lista de liberação, lista de bloqueio).

4.35. Validação com entradas digitais associadas

Deve ser possível associar o sinal de uma entrada digital na validação de acesso. Assim, a pessoa somente terá acesso permitido se depois da validação de suas informações o sinal das entradas digitais for igual ao sinal default que as entradas tem configuradas.

- Caso o estado de qualquer uma das entradas digitais associadas à validação de acesso seja diferente do estado default no momento da validação o firmware deve negar o acesso gerando evento de bloqueio pela entrada digital. Deve exibir no display a mensagem para o tipo de evento e logar a validação.

4.36. Desistência de acesso

Em dispositivo com catraca, após a validação de acesso, se o firmware não perceber o início do giro da catraca no tempo definido para executar o acionamento o firmware deve bloquear a catraca e considerar uma desistência de acesso.

- Caso a pessoa seja selecionada para revista aleatória o evento de desistência deve ser "Desistência de acesso - Revista aleatória" para indicar que a desistência foi feita após a pessoa ser sorteada.

4.37. Tipo de pessoa

Deve controlar o tipo de pessoa conforme o Validar Acesso:

- Controle de tipo de pessoa.
- Deve utilizar as informações do tipo de crachá ao invés das informações da pessoa.

4.38. Burla de catraca

Em dispositivos com catraca, se após a validação de acesso o firmware perceber o início do giro da catraca dentro do tempo de acionamento, porém não percebe o giro completo dentro do tempo de acionamento o firmware deve considerar como sendo uma burla de catraca.

4.39. Tempo mínimo de permanência

Deve ser controlado o tempo mínimo de permanência do mesmo modo que no DFS.

- Tempo mínimo de permanência.
- Configuração por pessoa.

4.40. Controles off-line para validação de acesso

Sempre que o firmware estiver off-line e ocorrer um dos eventos listados abaixo:

- Desistência de acesso (Pessoa teve o acesso válido, mas não girou a catraca).
- Acesso negado pela conferência biométrica (Pessoa colocou o dedo errado no momento da validação de biometria).
- Acesso negado pela conferência da senha (Pessoa digitou a senha incorreta).
- Desistência biométrica (Pessoa não colocou o dedo quando solicitada a biometria).
- Negado pela entrada digital (No caso de porta eclusa, quando a outra porta ainda não está fechada).

O firmware deve guardar em memória como estavam as informações da pessoa antes da validação do acesso. As informações que o firmware deve guardar são:

- Data e hora da ocorrência do evento (dd/mm/aaaa hh:mm:ss).
- Crachá (número físico).
- Nível onde a pessoa estava (origem).
- Consumo de crédito de acesso (Quantidade e faixa).
- Exibição de mensagem (Quantidade de exibições).
- Data e hora da última saída (Utilizada para intervalo de almoço e interjornada).
- Data e hora da última atualização do Smart Card.

Caso um crachá que está nesta lista passe no dispositivo o firmware deve comparar a data/hora de último acesso e a data/hora da última atualização do crachá com as datas registradas em memória, sendo que se a data/hora do último acesso e a data/hora da última atualização forem iguais as respectivas datas armazenadas no dispositivo o firmware deve utilizar todas as informações armazenadas no dispositivo para a validação de acesso ao invés das informações do crachá. Caso contrário deve utilizar as informações do crachá.

Observação Importante: Este controle deve ser feito pois o crachá Smart Card é atualizado no momento da validação e no caso de ocorrência dos eventos acima o crachá não está mais na leitora para que seja feita a gravação retornando os valores iniciais, antes da validação do acesso. Assim, conferência das informações deve ser feita na próxima passagem off-line no mesmo dispositivo.

Outras considerações:

- Deve guardar apenas os últimos 10 registro off-line ocorridos (limitados pelos eventos listados acima).
- Caso o firmware seja iniciado as informações armazenadas em memória, para atendimento deste requisito, devem ser apagadas.
- Este controle é aplicado somente para crachás de tecnologia Smart Card.

4.41. Validação com biometria 1:1

O firmware deve conseguir realizar validação de acesso com biometria 1:1.

- O firmware deve validar o acesso da pessoa e depois verificar se a pessoa é quem diz ser, solicitando a biometria no sensor biométrico. Se passar mais de 6 segundos após o firmware solicitar a biometria e a pessoa não apresentou a biometria o firmware deve considerar como uma desistência de acesso com biometria.
- O firmware deve configurar o leitor biométrico com o nível de conferência da pessoa antes de realizar a validação 1:1. Caso o firmware não consiga obter o nível de conferência biométrico da pessoa deve utilizar o nível padrão do sensor.

- Se o sensor informar que a pessoa não é quem diz ser o firmware deve negar o acesso pela conferência biométrica.

- O firmware deve verificar se o tipo de biometria que a pessoa apresenta na validação é o mesmo armazenado, inclusive comparando se o fabricante do sensor é o mesmo. Se não for deve negar o acesso pela conferência biométrica.

- Caso o firmware não consiga obter a biometria da pessoa deve negar o acesso da pessoa com a mensagem "Negado Biometria".

- Caso no retorno da validação de acesso não envie a biometria de uma pessoa que valide biometria ou no caso de uso de smart card onde o mapa Smart possua o campo de template de biometria, mas a biometria não está gravada no smart card, deve proceder da mesma forma que o requisito Pessoas sem templates.

4.42. Validação com biometria 1:N

O firmware deve conseguir realizar validação de acesso com biometria 1:N.

- O firmware deve perceber quando existe uma biometria no sensor biométrico e então comparar a biometria captada no sensor com as biometrias armazenadas anteriormente. Caso seja encontrada uma correspondência o firmware deve identificar a pessoa e realizar a validação de acesso com base nas informações da pessoa identificada.

- Caso não seja encontrada uma correspondência o firmware deve negar o acesso com a mensagem "Usuário não cadastrado" deixando a tentativa de acesso registrada em log.

- Caso ocorra alguma inconsistência durante a leitura da biometria da pessoa o firmware deve negar o acesso e exibir a mensagem "Acesso negado - Erro de leitura" deixando a tentativa de validação registrada em log.

4.43. Contingência da biometria

Deve ser possível configurar a ação a ser tomada quando o firmware não conseguir obter a biometria para realizar a validação 1:1. As opções possíveis são a de negar o acesso ou de realizar o acesso somente com as informações do crachá e/ou da pessoa.

4.44. Pessoa sem templates

Caso a pessoa valide biometria 1:1 e não possua templates o firmware deve negar o seu acesso gerando o evento de negado biometria e deve escrever no display do dispositivo a mensagem “Sem Templates biométricas”.

- Para crachás de tecnologia Barras e RFID essa situação somente deve ser controlada quando on-line.

- Para crachás do tipo Smart Card essa condição deve ser controlada quando on-line e off-line.

- O evento de acesso deve indicar que a pessoa não possui templates biométricos.

- Caso o dispositivo não possua display, deve apenas gera o evento.

4.45. Pessoa com template inválido

Caso a pessoa valide biometria 1:1 e não seja possível gravar o template no sensor biométrico, resultando em erro, o firmware deve negar o seu acesso gerando o evento de negado biometria e deve escrever no display do dispositivo a mensagem “Erro gravando templates”.

- Para crachás de tecnologia Barras e RFID essa situação somente deve ser controlada quando on-line.

- Para crachás do tipo Smart Card essa condição deve ser controlada quando on-line e off-line.

- O evento de acesso deve indicar que a biometria do crachá está inválida.

- Caso o dispositivo não possua display, deve apenas gerar o evento.

4.46. Obtenção da biometria

Para a validação biométrica 1:1 o firmware deve obter a biometria da seguinte forma:

- Quando on-line deve buscar a pessoa associada ao crachá e validar a biometria com base nesta pessoa.

- Quando off-line e o crachá for barras ou RFID: O firmware deve procurar a pessoa associada ao crachá e validar a biometria com base nesta pessoa. Se não encontrar a pessoa deve responder com acesso negado pela biometria.

- Quando off-line e o crachá for smart card o firmware deve buscar o template gravado dentro do crachá e enviar este template para o sensor comparar com a biometria apresentada pela pessoa. Caso não tenha biometria no crachá o firmware deve buscar a pessoa associada ao crachá e validar a biometria com base nesta pessoa.

4.47. Uso do display

Em dispositivos que possuem display a validação de acesso deve exibir mensagem para a pessoa sobre o andamento e o resultado da validação de acesso.

- Ao iniciar a validação deve exibir "Validando acesso".

- Ao atualizar o crachá deve exibir "Aguarde atualizando".

- Ao encerrar a validação do acesso deve exibir a mensagem correspondente ao evento (Acesso permitido ou um dos tipo de acesso negado).

- Deve ser possível exibir a data e hora, o número de matrícula e o sentido da liberação de acesso no resultado da validação de acesso.

- Caso seja configurado para exibir o número de matrícula e o firmware não tenha a informação deve exibir o número do crachá no lugar do número de matrícula.

- Não deve permitir combinar mensagens (resultado do evento, data e hora, número de matrícula) além da capacidade de exibição do display do dispositivo.

4.48. Utilização de urna / cofre coletor

Deve ser possível realizar a validação de acesso utilizando cofre coletor.

- Caso seja crachá Smart a validação é feita pela leitora Smart Card da urna. A abertura do cofre coletor deve ser feita após a validação do crachá, independente de acesso válido ou acesso negado.

- Caso o crachá seja de tecnologia diferente da tecnologia do smart card, deve ser possível validar o acesso apenas depositando o crachá na urna.

- Deve ser possível operador de segurança configurar o tempo de espera para abertura do cofre e o tempo em que o cofre deve permanecer aberto.

- Deve ser possível a utilização da urna para todos os tipos de tecnologia de crachá, de modo on-line e off-line, ou seja, se o dispositivo estiver configurado para solicitar urna, deve solicitar tanto quando estiver on-line e quando off-line.

4.49. Digitação de função

Deve ser possível digitar uma função durante a validação de acesso.

- A função digitada deve ser enviada juntamente com o evento de acesso gerado.

- Exceção: Funções que realizam operações específicas não devem ser enviadas com o evento de acesso.

4.50. Início e fim da validação

A validação de acesso deve iniciar quando o firmware detectar a presença de um crachá ou biometria em uma de suas leitoras. A validação de acesso deve ter um dos resultados seguintes:

- Acesso válido.

- Acesso negado.

- Desistência de Acesso.

- Erro de leitura.

4.51. Criptografia de crachás

O firmware deve suportar os seguintes tipos de criptografias de crachás de barras:

- Criptografia Telemática: Deve receber da aplicação a chave de descriptografia e o tipo de algorítimo correspondente. Deve utilizar a chave para descriptografar o número lido na leitora conforme o tipo de algorítimo.

- Criptografia Senior: Deve receber da aplicação a chave de descriptografia e utilizar esta chave para descriptografar o número lido na leitora conforme o algorítmo Senior.

- Sem criptografia: Utiliza a máscara. Deve-se verificar na configuração do dispositivo quais dígitos devem ser utilizados e quais devem ser descartados.

- O tamanho da máscara é de 25 dígitos.

- A quantidade máxima de dígitos aproveitados na máscara é de 12 dígitos.

- Após ser discriptografado o número do crachá deve ter no máximo 12 dígitos.

4.52. Gravação do Smart Card

A gravação do Smart Card completo deve ser feita no máximo em 1.500 (mil e quinhentos) milissegundos.

4.53. Timeout de validação na DFS

O timeout de validação no DFS é de 2.000 milissegundos. Caso a validação demore mais que o tempo de timeout o firmware deve realizar a validação de acesso com as informações do crachá e atualizar o seu Status para off-line.

4.54. Tempo de validação Off-line

O tempo de validação de acesso off-line deve ser inferior a 800 milissegundos.

4.55. Margem de erro da revista aleatória

A revista aleatória deve ter margem de erro aceitável de até 10% em relação ao percentual configurado.

Exemplo:

Tipo crachá - % Configurado - Margem de erro (de /até)

Empregado - 20% - de 18% até 22%
Aluno - 15% - de 16,5% até 17,5%
Visitante - 5% - de 4,75% até 5,25%

Observação: A verificação deve ser feita com uma base de pelo menos 1000 pessoas de cada tipo durante uma semana. Sábado e domingo devem possuir um volume diferenciado de pessoas passando. Sábado um volume 50% menos que durante a semana e domingo um

volume 70% menos que durante a semana. A margem de erro deve ser calculada por dispositivo.

5. Eventos

Enviar os eventos de acesso e alarmes ocorridos no dispositivo para o driver e gravá-lo localmente também.

5.1. Monitoramento das entradas digitais

O firmware deve monitorar as entradas digitais configuradas e gerar evento de alarme toda vez que o estado da entrada digital for alterado.

- Os eventos de alarme devem conter uma indicação se o alarme foi ativado ou desativado. Essa indicação é calculada com base no estado original da entrada digital, sendo:
- Se o estado original for "desativado", e a entrada for "acionada", o evento de alarme é "Ativo".
- Se o estado original for "desativado", e a entrada for "liberada", o evento de alarme é "Inativo".
- Se o estado original for "ativado", e a entrada for "acionada", o evento de alarme é "Inativo".
- Se o estado original for "ativado", e a entrada for "liberada", o evento de alarme é "Ativo".
- Deve gerar alarme ao sair do estado default e ao retornar ao estado default.
- Deve ser possível configurar um tempo de espera para geração do evento de alarme. Por exemplo, se configurado o tempo de espera em 5 segundos, um alarme de uma entrada digital somente será criado após passar 5 segundos da ativação sem retornar ao estado default.

5.2. Entradas digitais dependentes

O firmware não deve gerar evento de alarme para mudança de estado de uma entrada digital dependente.

- Para gerar evento de alarme em uma entrada digital dependente deve-se configurar o tempo de monitoramento fora do estado padrão (*default*). Após a entrada digital ser ativada ou desativada, se passar o tempo de monitoramento e a entrada digital não retornar ao estado padrão o firmware deve gerar um evento de alarme conforme requisito Monitoramento das entradas digitais.

5.3. Dispositivo alarmado

O evento de alarme deve escrever "ALARMADO" no display quando a configuração indicar que tal entrada digital usa display. O tempo de escrita no display será igual ao tempo que o alarme estiver ativo, ou seja, quando a entrada digital voltar ao estado original o display irá retornar ao normal.

5.4. Evento mascarado

Deve ser possível configurar um período de mascaramento de evento de alarme.

- O período de mascaramento deve ter hora inicial e hora final do mascaramento juntamente com a entrada digital mascarada. Caso não seja informado um dos valores não deve executar o mascaramento de eventos de alarme.

- Todo evento gerado pela entrada digital mascarada, durante o horário do mascaramento deve ter um assinalamento informando que o evento foi gerado durante um período de mascaramento de alarme.

5.5. Burla de catraca

Em dispositivos que possuem catraca firmware deve possuir configuração de tempo para monitoramento do giro da catraca. O valor default para o tempo de monitoramento do giro da catraca deve ser zero (0), indicando que não monitora o giro da catraca.

- Caso o tempo de monitoramento seja maior que zero, o firmware deve verificar quando o giro da catraca foi iniciado. Se o giro da catraca não for completado antes do tempo configurado para monitoramento o firmware deve gerar um evento de acesso de burla de catraca, indicando o crachá que teve o acesso válido que originou a liberação do giro da catraca.

5.6. Desistência de acesso

Para dispositivos que possuem catraca, o firmware deve possuir configuração de tempo máximo de validação de acesso. Após um acesso válido com liberação da catraca o firmware deve verificar se a catraca iniciou o giro. Caso passe mais tempo que o tempo configurado para desistência de acesso o firmware deve bloquear a catraca e gerar um evento de desistência de acesso informando o crachá que teve o acesso válido gerado da liberação da catraca.

5.7. Evento de acesso

O firmware deve gerar evento de acesso para toda solicitação de acesso feita no dispositivo.

- O evento de acesso deve identificar o crachá ou a pessoa que solicitou o acesso. Caso não seja possível identificar nem o crachá nem a pessoa o firmware não deve gerar evento de acesso.

- Para acessos negados o firmware deve identificar no evento de acesso a causa da negação do acesso.

- Deve identificar se o evento ocorrer quando o firmware estava on-line ou quando esta off-line em relação à aplicação.

- Em caso de acesso permitido o evento deve informar se a pessoa foi sorteada para revista aleatória.

5.8. Direção do acesso

O firmware deve indicar a direção do acesso nos eventos de acesso válido.

- Em dispositivos que controlam apenas um sentido a direção do acesso deve ser sempre no sentido configurado na leitora.

- Em dispositivos que controlam ambos os sentidos e possuem giro de catraca deve indicar a direção do acesso pelo sentido do giro da catraca.

- Em dispositivos que controlam ambos os sentidos e não possuem giro de catraca e nem controle de nível deve indicar a direção do acesso adotando a direção configurada da origem para o destino.

- Em dispositivos que controlam ambos os sentidos e nível, deve adotar a direção conforme o nível para onde a pessoa é liberada.

5.9. Dispositivo fora do estado de repouso

Se ao realizar um acionamento em decorrência de um acesso válido o firmware detectar que a saída digital já está acionada deve gerar um evento de acesso informando que o dispositivo está fora do estado de repouso.

5.10. Intrusão

O firmware deve notificar ao sistema quando houver uma instrusão. A intrusão ocorre sempre quando o acesso é feito sem ter ocorrido previamente uma validação.

5.11. Envio do evento

Todo evento gerado deve ser enviado para o DFS.

- Caso não tenha comunicação com o DFS o firmware deve armazenar o evento até que seja estabelecida a comunicação.

- Caso no momento da gravação do evento o arquivo que armazena os eventos não enviados estiver com a capacidade total ocupada o firmware deve bloquear todas as leitoras até que consiga enviar os eventos.

5.12. Persistência dos eventos

O firmware deve persistir todos os eventos ocorridos, diferenciando os que já foram enviados para o DFS, os que não foram enviados e os que foram enviados mas, não foram recebidos.

- Caso não tenha mais espaço físico para gravar os eventos não **recebidos pelo DFS**, o firmware deve bloquear todas as suas leitoras configuradas. O motivo de bloquear o dispositivo é evitar que qualquer evento não entregue seja perdido.

- Os eventos já enviados podem ser regravados para aproveitar o espaço físico, conforme requisito Limites de eventos enviados.

5.13. Eventos com informações cadastradas

Os eventos que contenham informações cadastradas (biometria) devem ser armazenados com as informações anexas.

- Após receber confirmação de que o sistema recebeu o evento com informações cadastradas o firmware deve excluir a informação anexa ao evento para liberar espaço físico.

5.14. Capacidade de armazenamento de eventos

O firmware deve avisar o usuário sobre a capacidade de armazenamento de eventos.

- Quando o firmware estiver com menos de 10% ou de sua capacidade de armazenamento de eventos, o firmware deve exibir um sinal visual ao usuário no display do dispositivo, caso o dispositivo possua display. O sinal visual de capacidade abaixo de 10% é um caracter "!". O firmware deve também gerar um evento de alarme indicando que a capacidade de armazenamento de eventos está abaixo de 10%.

- Quando o firmware estiver com 100% de sua capacidade de armazenamento esgotada, o firmware deve exibir um sinal visual ao usuário no display do dispositivo, caso o dispositivo possua display. O sinal visual de capacidade de armazenamento esgotada é um caracter "*". O firmware deve também gerar um evento de alarme indicando que a capacidade de armazenamento de eventos está esgotada.

- Caso a capacidade de armazenar eventos no firmware seja esgotada o firmware deve bloquear todas as suas leitoras impedindo a validação de acesso. Caso possua display deve exibir no display a mensagem "Bloqueado".

- Deve logar sempre que a capacidade de armazenamento ficar inferior a 10%, sempre que a capacidade de armazenamento for esgotada e quando conseguir liberar espaço para armazenamento dos eventos.

5.15. Limite de eventos enviados

O firmware deve gerenciar eventos que já enviados ao sistema.

- Após o envio e a confirmação de recebimento, o evento deve ser armazenado no firmware em um local próprio para os eventos enviados.

- Caso a capacidade de armazenamento de eventos seja alcançada, os eventos mais antigos devem ser descartados para liberar espaço.

6. Biometrias

Ler a biometria da pessoa através das leitoras biométricas. Realizar o cadastramento da biometria.

Embora este caso de uso tenha interface com o usuário esta interface é através de dispositivos construídos pela Digicon. Com base nisso não tem sentido em construir protótipos.

6.1. Cadastro de digitais Sagem

Ao cadastrar digitais em um sensor *Sagem* o dispositivo deve solicitar 2 (duas) digitais distintas para a pessoa.

- O firmware deve solicitar uma digital de cada vez, exibindo no display a mensagem "Apresente 1° dedo (3 vezes)" para a primeira digital e "Apresente o 2° dedo (3 vezes)" para a segunda digital.

- Caso a pessoa demore mais de 6 segundos para apresentar a digital o firmware deve cancelar o cadastro e exibir no display a mensagem "Cadastro cancelado".

6.2. Capacidade suporte para Sagem

Deve ser possível configurar a capacidade do sensor biométrico Sagem. A configuração deve respeitar os limites técnicos do fabricante, sendo:

- 500 usuários
- 3000 usuários
- 5000 usuários

Cada usuário deve possuir duas templates.

O Firmware não deve fazer consistência entre a capacidade configurada e a capacidade real do sensor, mas deve acusar erro caso tente incluir uma nova biometria e a capacidade do sensor já estiver esgotada (A justtificativa para este requisito é que o fabricante não possui interface disponivel que informe a capacidade de armanzenamento).

Observação: A responsabilidade de indicar a capacidade do sensor biométrico é do fabricante do dispositivo, neste caso, a Digicon.

6.3. Capacidade do sensor Suprema

Deve ser possível configurar a capacidade do sensor biométrico Suprema.

- Cada usuário cadastrado no sensor deve possuir uma templates.

O Firmware não deve fazer consistência entre a capacidade configurada e a capacidade real do sensor, mas deve acusar erro caso tente incluir uma nova biometria e a capacidade do sensor já estiver esgotada (A justtificativa para este requisito é que o fabricante não possui interface disponivel que informe a capacidade de armanzenamento).

Observação: A responsabilidade de indicar a capacidade do sensor biométrico é do fabricante do dispositivo, neste caso, a Digicon.

6.4. Cadastro de biometria Suprema

Ao cadastrar digitais em um sensor *Suprema* o dispositivo deve solicitar 2 (duas) digitais distintas para a pessoa.

- O firmware deve solicitar uma digital de cada vez, exibindo no display a mensagem "Apresente 1° dedo (2 vezes)" para a primeira digital e "Apresente o 2° dedo (2 vezes)" para a segunda digital.

- Caso a pessoa demore mais de 6 segundos para apresentar a digital o firmware deve cancelar o cadastro e exibir no display a mensagem "Cadastro cancelado".

6.5. Espaço reservado para validação de acesso

O Firmware deve manter espaço suficiente no sensor biométrico para realizar a validação de acesso.

- Deve ser mantido espaço no sensor para que seja possível gravar pelo menos um conjunto de templates necessários para a validação do acesso.

- Sempre que necessitar liberar espaço do sensor para inclusão de novos templates o firmware deve excluir as templates do usuário que está a mais tempo sem usar a biometria.

6.6. Cadastro de Handkey Recognition System

Ao cadastrar handkey em um sensor *Recognition Systems* o dispositivo deve solicitar que a pessoa apresente 3 (três) vezes a mão direita.

- O firmware deve exibir no display a mensagem "Coloque a mão direita" para a primeira solicitação damão e nas seguintes deve escrever "Coloque a mão 2/3" e "Coloque a mão 3/3" respectivamente.

- Caso a pessoa demore mais de 30 segundos para apresentar a mão o firmware deve cancelar o cadastro.

6.7. Restrições do cadastro de biometria

Deve ser possível cadastrar templates biométricas nos dispositivos, desde que:

- O dispositivo possua um sensor biométrico associado.
- A funcionalidade de cadastro de biometria esteja ativa.
- O sensor biométrico tenha capacidade de armazenar novas biometrias.

- O dispositivo possua display.

6.8. Ativação do cadastro

Deve ser possível ativar/desativar o cadastro de biomeria no dispositivo das seguintes maneiras:

- Comando que configura a funcionalidade de cadastro de biometria.

A ativação do cadastro de biometria está vinculado as condições descritas no requisito Restrições de cadastro de biometrias.

6.9. Cadastro da biometria

Deve ser possível cadastrar uma coleção de templates biométricos para uma pessoa em um sensor do dispositivo.

- O firmware deve identificar a pessoa no momento do cadastro da biometria. Caso o firmware não consiga identificar a pessoa deve impedir o cadastro da pessoa exibindo a mensagem "Pessoa não identificada". Caso o firmware esteja on-line, deve solicitar a identificação da pessoa para o DFS caso não consiga identificar a pessoa por sí próprio.

- O sensor e o firmware devem possuir capacidade suficiente para armazenar os templates cadastrados. Caso o sensor ou o firmware não possam armazenar os templates da pessoa, o firmware deve exibir no display a mensagem "Cadastro negado. Memória cheia".

- Após a identificação da pessoa o firmware deve solicitar o cadastramento dos templates de acordo com o funcionamento de cada tipo de sensor biométrico.

- Ao concluir o cadastro da biometria da pessoa o firmware deve exibir no display a mensagem "Templates cadastradas" e gerar um evento de template cadastradas, identificando a pessoa que cadastrou as templates.

6.10. Gravação de SmartCard

Caso o crachá da pessoa utilizado para o cadastro da biometria seja Smart Card, o firmware deve atualizar as templates cadastradas no crachá.

- O firmware deve solicitar ao usuário que aproxime o crachá da leitora smart card. Caso o usuário não aproxime o crachá em 6 (seis) segundos o firmware deve cancelar o cadastro da biometria e exibir a mensagem "Cadastro cancelado" no display do dispositivo.

- Caso o crachá apresente erro na gravação dos templates o firmware deve executar o procedimento de gravação novamente, até o limite de 3 (três) vezes. Se ao final de todas as tentativas o firmware não conseguir gravar o cracha deve cancelar o cadastro das templates e exibir no display a mensagem "Cadastro cancelado".

- Caso não seja possível gravar as duas templates no Smart Card em função da falta de espaço, o firmware deve gravar apenas a primeira template cadastrada. Caso não tenha espaço para gravar nenhuma das templates o firmware deve cancelar a gravação do Smart Card. Não deve cancelar o cadastro das templates.

Observações:

- Quando o requisito menciona duas templates, significa as duas templates da mesma tecnologia biométrica, ou seja, duas templates *Sagem* ou duas templates *Suprema*.

- Caso não tenha espaço no crachá para gravar a template o firmware não exibe mensagem para o usuário para não induzir ao erro. Caso fosse exibida uma mensagem como por exemplo "Falta de Espaço. Templates não Gravadas" iria induzir o usuário a recadastrar indefinidamente a sua biometria.

6.11. Erro no cadastro

Caso o equipamento apresente algum erro ao cadastrar a biometria o dispositivo deve apresentar no display do equipamento a mensagem "Erro ao cadastrar biometria" e cancelar o cadastro.

6.12. Fabricantes suportados

O Firmware deve permitir o cadastro de biometrias digitais dos fabricantes:

- Sagem
- Suprema
- HandKey

Se por qualquer motivo for enviada alguma biometria de outro fabricante ou tipo para o firmware o firmware deve recusar a templates indicando em seu log que a biometria é desconhecida.

Observação: Neste caso pode ser que o firmware não responda com erro, pois, ele pode não conhecer a interface que está enviando a template. Exemplo: A Digicon pode criar suporte em sua LIB para um novo fabricante de biometria e um cliente começar a utilizar. O Firmware não tem obrigação de avisar para a LIB digicon que está ocorrendo erro, porém deve registrar em seu log que a biometria é desconhecida.

6.13. Templates já existentes

Caso a template cadastrada já exista no sensor associada a outra pessoa o firmware deve cancelar o cadastro e exibir a mensagem "Template já cadastrada" no display.

6.14. Validação de acesso

Mesmo permitindo incluir templates o firmware deve garantir a execução da validação de acesso 1:1 quando estiver configurado com esta funcionalidade.

O firmware não deve permitir cadastrar templates caso isso impeça uma validação de acesso 1:1, conforme requisito Restrições do cadastro da biometria.

6.15. Armazenamento das templates

O firmware deve manter todas as templates cadastradas até que receba confirmação da aplicação de que as templates foram gravadas na base de dados.

- Caso seja necessário liberar espaço para inclusão de novas templates, o firmware somente pode excluir templates que já foram gravadas na base de dados da aplicação.

6.16. Atualização de biometria

Deve ser possível atualizar os templates de uma pessoa no sensor biométrico. As opções de atualização de templates são:

- Exclusão de template do sensor
- Inclusão de template no sensor
- Alteração de template no sensor

6.17. Quantidade máxima de usuários/templates

O firmware não deve permitir incluir mais usuários e templates do que a capacidade do sensor biométrico.

- Caso algum comando ordene a inclusão de mais usuários ou mais templates do que a capacidade do sensor, o firmware deve recusar a inclusão retornando erro de capacidade de sensor.

7. Inicialização

Indicar para o sistema que um novo dispositivo foi instalado na rede e fazer o novo dispositivo se comunicar com o sistema.

7.1. Condição de inicialização

O Loader deve ser executado automaticamente caso o dispositivo não possua firmware.

- Caso possua firmware o loader não deve ser executado de forma automática, mas, deve ser possível a execução através de linha de comando, para que seja possível executar a rotina de testes da Digicon

- O Loader não deve executar caso o firmware esteja executando, assim, para a execução via linha de comando o firmware deve ser encerrado.

7.2. Opções de menu

Ao executar o loader deve exibir um menu para o usuário com as seguintes opções:

- 1-Execução de testes
- 2-Configuração via rede
- 3-Atualização off-line

7.3. Execução de teste

Caso seja secionada a opção 1 do menu, o Loader deve chamar a rotina de testes disponibilizada pela Digicon.

Observação - Após a chamada da rotina de teste o controle do equipamento não é mais de responsabilidade do Loader. Somente após finalizada a rotina de testes que o Loader volta a ser responsável pelo controle do dispositivo.

7.4. Configuração de rede

Ao ser selecionado a configuração via rede (2) o Loader deve solicitar as informações abaixo, na mesma ordem em que são apresentadas:

1 - Identificador do dispositivo
2 - Tipo de IP: A - Fixo ou B - DHCP
3 - IP do dispositivo
4 - Máscara de rede
5 - Gateway da rede
6 - IP do servidor
7 - Porta de comunicação do servidor

- O identificador do dispositivo pode ser zero, porém neste caso vai apenas atualizar o firmware do dispositivo, sem solicitar a configuração.

- As informações 3, 4 e 5 só devem ser solicitadas caso seja escolhida a opção A no itém 2, ou seja, somente de ve solicitar o IP do dispositivo, a máscara e o gateway da rede caso o IP seja fixo.

- Para todo número de IP digitado deve ser feita a conferência do número e avisar caso o IP seja inválido.

- O IP do servidor não pode ser zero.

- A porta de comunicação não pode ser zero.

- Não deve solicitar a próxima informação enquanto existir inconsistência na informação atual.

- Caso seja pressionada a tecla ESC na MCAnet ou ANULA na MCA o loader deve cancelar as operações e retornar ao menu.

Observação: Ao finalizar a configuração o Loader deve conectar-se no aplicativo e porta configurados e aguardar o envio do firmware.

7.5. Atualização off-line

Ao ser selecionada a opção de atualização off-line (3), o Loader deve solicitar que seja inserido um pendrive na porta USB. Quando detectar que foi inserido um pendrive o Loader deve verificar a existência do arquivo firmware.tar.gz no diretório raiz do pendrive.

- Caso não seja localizado o arquivo firmware.tar.gz no diretório raiz do pendrive o Loader deve exibir a mensagem "Firmware não localizado".

- Caso seja pressionada a tecla ESC na MCAnet ou ANULA no caso da MCA o Loader deve cancelar as operações e retornar ao menu.

- Após verificar que o o arquivo firmware.tar.gz existe, o Loader deve copiar o arquivo e executar o arquivo.

8. Acionamentos

Este caso de uso descreve como deve ser o gerenciamento de todos os acionamentos que o firmware executa.

Os acionamentos podem ser executados após uma validação de acesso, via comando vindo da aplicação ou podem ser programados para executarem em determinado dia e horário.

8.1. Ativação de emergência

Quando estiver em emergência o firmware deve executar os acionamentos configurados para o estado de emergência.

- Em dispositivos que possuem catraca o firmware deve liberar o giro quando estiver em estado de emergência, sem gerar eventos de acesso.

8.2. Ativação de emergência com crachá mestre

Deve ser possível ativar e desativar o estado de emergência de um dispositivo com a utilização do crachá mestre associado a digitação de uma função específica.

- O crachá deve ter acesso válido.
- Após a ativação da função de emergência deve aguardar 5 segundos até a passagem do crachá mestre, caso o crachá não seja passado deve cancelar a ativação.
- Caso o dispositivo esteja com estado de funcionamento normal, ou seja, sem emergência, a função pressionada deve ativar a emergência.
- A desativação do estado de emergência deverá ser feito por comando.
- Na ativação do estado de emergência deve escrever no display "Emergência".
- A função para ativação de emergência deve ser configurável, ou seja, o usuário pode escolher qual a função utilizada para esta finalidade.

Observação: A desativação do comando de emergência não pode ser feita pelo crachá mestre e função pois o teclado e as leitoras ficam bloqueadas quando o dispositivo está em emergência.

8.3. Acionamentos possíveis

Deve ser possível acionar os seguintes periféricos controlados pelo firmware:

- Saída digital
- Display
- Pictograma
- Buzzer
- Giro de Catraca / torniquete
- Urna
- Solenóide
- Led verde e led vermelho da leitora

Não deve ser permitido o acionamento de solenóide quando utilizado o giro de catraca.

8.4. Acionamentos programados

Deve ser possível executar acionamentos do firmware de forma programada.

- Deve ser possível programar acionamentos para execução de tempos em tempos. Exemplo: Executar a cada duas horas.
- Deve ser possível programar acionamentos para execução em determinado horário. Exemplo: Executar sempre as 13:30
- Deve ser possível informar tipos de dias para o acionamento ser ou não executado. Ex: Domingo, Feriados, Sexta-Feira.
- Deve ser possível informar um período para execução dos acionamentos. Os acionamentos serão executados somente durante o período definido. Exemplo: Executar entre 01/06/2009 as 14:00 até 30/06/2009 as 18:00.
- Deve ser possível indicar a quantidade de vezes que o acionamento deve ser executado.
- Deve ser possível consultar os acionamentos programados e a data da próxima execução programada para o acionamento e a data da última execução.
- Deve ser possível excluir os acionamentos programados. Neste caso deve excluir todo o conjunto de acionamentos e não apenas uma ocorrência do acionamento.

8.5. Acionamentos por eventos

Deve ser possível configurar acionamentos para execução em acessos válidos, acessos negados e para eventos de alarme.

- O acionamento deve ser configurado pelo tipo de eventos.
- Para eventos de alarme deve ser possível o controle de giro de catraca, porém não será possível fazer apenas um giro. O giro deverá ficar liberado por um tempo determinado ou até que o alarme retorne ao estado default, o que for maior.

8.6. Tempo de acionamento

Todo acionamento deve possuir um tempo de acionamento que informe durante quantos milisegundos que o acionamento deve ser mantido.

- Caso este valor seja zero o acionamento não deve ser desligado.
- Deve ser possível interromper um acionamento já iniciado.
- Para acionamentos em conjunto que contenham mensagens, o tempo de exibição da mensagem deve ter o mesmo valor do tempo do maior acionamento.
- No caso de dispositivos com catraca, assim que o giro for completo os acionamentos de acesso devem ser interrompidos.

8.7. Entradas digitais

Deve ser possível configurar acionamentos para as entradas digitais.

- Os acionamentos devem ser executados quando o valor padrão da entrada digital for alterado e devem ser finalizados quando a entrada digital voltar ao valor padrão.

- Se a entrada digital estiver em período de mascaramento não deve gerar acionamento, conforme requisito Acionamento de alarmes.

8.8. Restrições de acionamentos

Somente podem ser acionados periféricos que o dispositivo tem instalado. Caso seja acionado um periférico que o dispositivo não possua pode gerar um erro de execução. Caso gere um erro na execução o firmware deve logar o erro.

8.9. Acionamentos de revista aleatória

Deve ser possível configurar acionamentos para a revista aleatória. Os acionamentos configurados para a revista aleatória serão executados quando uma validação de acesso retornar que a pessoa foir sorteada para a revista.

- Juntamente com os acionamentos da revista aleatória o firmware deve executar os acionamentos do tipo de acesso, seja acesso válido ou acesso negado. Por exemplo, se o acionamento de acesso válido é o giro de catraca e o acionamento de revista aleatória é acionar a saída digital 2 (uma sirene), o firmware deve acionar ambos.

- Caso o tipo de acesso e a configuração da revista aleatória tenham os mesmo acionamentos, os acionamentos iguais serão executados apenas uma vez. Por exemplo, se tanto o acionamento de acesso válido quanto o de revista aleatória acionam o giro de catraca, somente um giro deve ser acionado, sem permitir que a catraca seja girada duas vezes.

- Caso o tipo de acesso e a configuração da revista aleatória tenham acionamentos conflitantes, o firmware deve executar os acionamentos configurados para a revista aleatória. Por exemplo, se o acesso permitido tem configurado para escrever no display "Acesso permitido" e a revista aleatória tem configurado para escrever "Revista aleatória", o display deve exibir "Revista aleatória".

8.10. Mascaramento de entradas digitais

Deve ser possível configurar horários em que as entradas digitais não devem gerar acionamentos, ou seja, ficam mascaradas.

- Deve ser possível configurar faixas em que a mudança de estado da entrada digital não deve gerar acionamentos.

- Deve ser possível configurar até sete faixas por cada tipo de dia, sendo que os tipo de dia são: Dias úteis, sábados, domingos e feriados.

- O tipo de dia feriado sobrepõe qualquer outro tipo de dia.

- Acionamentos programados, acionamentos de acesso ou acionamentos de emergência não devem ser afetados pelo mascaramento.

- Se ao sair da faixa de mascaramento o estado da entrada digital estiver diferente de seu estado default os acionamentos devem ser executados normalmente.

9. Problemas, compreendendo e resolvendo

Mesmo com toda atenção e preocupação constante com nossos produtos, não estamos imunes de erros ou problemas.

Nosso processo de qualidade prevê melhoria contínua nos processos para desenvolvimento de produtos e serviços, neste sentido estamos abertos a críticas e sugestões.

Estamos trabalhando compilando informações sobre análise de erros e situações encontradas pelos usuários e em breve farão parte deste manual.

Para registrar criticas, sugestões e elogios, acesse no site:

http://www.digicon.com.br/site/pt/smrelacionamento.html

Se preferir enviar e-mail para: aliancas.vca@digicon.com.br

10. Histórico de revisões do manual

Versão	Data	Descrição
1.0	08/04/2012	Início da criação deste manual foi em 20/03/2012, estruturando 182 (cento e oitenta e dois) requisitos funcionais e não-funcionais em 7 (sete) casos de uso.
1.1	20/04/2012	Substituição do nome do manual de |"Manual Acesso" para "Manual SDK Acesso", pois será parte integrante do SDK. Correções de termos, siglas e seus significados. Reclassificação de alguns requisitos.

11. Glossário

- **Antipassback:** Antipassback também é conhecido como AntiDupla. Este controle evita as caronas e é feito controlando o ultimo acesso da pessoa. Se a ultima passagem do usuário foi de entrada ou de saída. Se foi de entrada o próximo acesso deverá ser de saída. Se foi de saída, o próximo acesso deverá ser de entrada. Normalmente isso é ocnfigurado por dispositivo e por pessoa e podem haver vários tipos de controle: Hard Antipassback, Soft Antipassbak e Reset AntiPassback.
- **Agrupador:** É um link e um sinalizador para local físico de nível hierárquico inferior. Embora agrupe locais físicos e dispositivos, não confundir com grupo de dispositivos.
- **Alarme Acidental (Acidental Alarm):** Refere-se ao recebimento de sinal cujo evento que, embora corresponda à realidade dos fatos, ocorre por descuido ou desconhecimento do usuário. Tal evento deve ser imediatamente comunicado pelo usuário à central de monitoração, com a finalidade de se cancelar a tomada de providências (alarm cancel), sob pena de enquadrar-se em infração prevista no Código Penal Brasileiro. Outros termos popularmente empregados: Disparo Falso; Alarme Provocado; etc.
- **Alarme Falso (False Alarm):** Refere-se ao recebimento de sinal cujo evento que não corresponde à realidade dos fatos. Pode ser motivado por problemas técnicos, má aplicação do produto (instalação em local impróprio ou venda inadequada), má utilização e conservação por parte do cliente (umidade de paredes, lavagem de componentes), agentes externos provocados no local por parte do cliente (animais soltos, aquecedores, ventiladores, ar cond. ligados), preparo inadequado do local antes de se armar o sistema (janelas abertas, portas encostadas ou entreabertas, cortinas soltas, etc.). Outros termos popularmente empregados: Disparo Falso; Disparo Imotivado; Alarme Imotivado; etc.
- **Alcance Nominal (Nominal Range):** O alcance em que sistemas podem assegurar para operação confiável, considerando a variabilidade normal do ambiente em que é usado.
- **Ambiente Controlado:** Ver Área Controlada.
- **APB:** Ver Antipassback.
- **API:** Application Programming Interface, bibliotecas ou camadas intermediárias, normalmente fazem parte do SDK.
- **Aplicação:** Principal componente de software da solução, contêm todas as interfaces com o usuário para cadastros, consultas, processos e relatórios.
- **Aplicativo:** Ver aplicação.
- **Arme_Desarme (arm_disarm):** Termo utilizado para o ato de se preparar o sistema para informar silenciosamente ou não uma possível violação ou intrusão em uma área internamente sensoreada pelos seus componentes detectores. Pode ser feito mediante o acionamento de um botão de controle remoto, digitação de um código numérico em um teclado digital, ou ainda através de dispositivos de controle de acesso (cartão magnético, proximidade, detector biométrico, etc.) (.....) Outros termos popularmente empregados: Ativação / Desativação; Liga / Desliga; etc.
- **Assinatura Digital:** Método de autenticação digital garantido a confiabilidade da fonte de informações.
- **AFD:** Termo da Portaria 1510. Significa "Arquivo-Fonte de Dados" e é gerado a partir dos dados armazenados na MRP. Este arquivo é obtido pelo fiscal do trabalho diretamente no REP através de porta fiscal.
- **AFDT:** Termo da Portaria 1510. Significa "Arquivo-Fonte de Dados Tratados", este é gerado a partir dos dados armazenados na MRP e alterações posteriores realizadas sobre os dados originais. Este arquivo é gerado e enviado eletrônicamente quando solicitado pelo auditor-fiscal do trabalho. Caso haja diversos REP's em um mesmo estabelecimento, será apresentado apenas um AFTD com registros relativos a todos os REP's.
- **Alarme de teste:** Alarme de teste é um sinal gerado por aparelhos ligados a entradas de controladores de acesso. Esses aparelhos fazem com que determinada entrada entre em curto de tempos em tempos, gerando assim um sinal de alarme. Caso o sistema não receba um sinal de teste gerado por este curto durante um tempo maior que o definido em "Intervalo do Alarme de Teste", um sinal chamado "Falha no Sinal de Alarme de Teste" é gerado pelo coletor de alarmes, buscando notificar que determinado coletor não enviou o sinal dentro do tempo esperado. Os

alarmes de testes são particularmente úteis para verificação de estabilidade de equipamentos, visto que quando o sistema não recebe um retorno do coletor com um alarme de teste, é identificado um problema de conexão com o equipamento controlador, alertando este fato diretamente no monitoramento de alarmes.

- **BDCC:** Banco de Dados Comum de Credenciamento. Serve para controle de pessoas e veículos em áreas sob jurisdição aduaneira. O BDCC é um sistema de armazenamento de informações congregando dados de identificação que centraliza um fluxo estimado em milhares de trabalhadores e veículos que acessam mais de uma centena de recintos alfandegados no complexo portuário de Santos e Guarujá, o maior da América Latina.
- **Biometria:** Ciência da aplicação de métodos de estatística quantitativa a fatos biológicos; análise matemática de dados biológicos. 2 Fisiol Doutrina científica e artística da medida do corpo humano Matrícula - a partir da captura ótica da impressão digital, é gerada um modelo matemático correspondente à imagem colhida. Este modelo é armazenado para posteriores autenticações. Autenticação (1 p/ 1)- Traduz-se pela pergunta: "Esta pessoa é quem diz ser?". A partir da captura ótica da impressão digital a ser autenticada, é gerado um modelo matemático correspondente à imagem colhida. Este modelo é comparado com o modelo previamente armazenado no processo de matrícula do indivíduo que solicita a autenticação. Esta operação é realizada por sofisticados algoritmos e quando a comparação atende aos parâmetros de acuricidade estabelecidos, o acesso é liberado. Seja ele lógico ou físico. Normalmente este processo leva menos de 1 seg.! Identificação (1 p/ n) - Traduz-se pela pergunta: "Você conhece essa pessoa?". A partir do modelo matemático da impressão digital a qual deseja identificar-se o indivíduo, é feita uma busca em toda a base de dados de modelos biométricos buscando-se aqueles que, dentro dos parâmetros de acuracidade estabelecidos, possam corresponder ao indivíduo a qual pertence a impressão digital coletada. Normalmente é utilizado em aplicações criminais e o tempo de resposta varia em função de uma série de fatores. É importante ressaltar que a imagem da impressão digital não é armazenada em nenhum momento, e também não é possível reconstituí-la a partir do modelo matemático que a representa, preservando-se assim a privacidade.
- **Biometria - índices:** Índices para medir a funcionalidade de um sistema biométrico de identificação e verificação: FAR FRR FER UMBRAL FTE Para saber mais sobre os índices, consulte cada um no glassário.
- **Burla de catraca:** Uma busla de catraca ocorre quando é iniciado um giro de catraca e este giro não se completa ou se completa com tempo maior que o definido para um giro normal.
- **Buzzer:** Dispositivo que gera aviso sonoro. O buzzer pode ser acionado por um tempo determiando e é utilizado para emitir um aviso sonoro para um tipo de validação de acesso, por exemplo.
- **Baixa automática do crachá:** O processo de baixa automática permite realizar a baixa automaticamente dos crachás de visitantes, acompanhantes ou integrante de grupos sem que seja efetuada a saída do visitante pelo sistema.
- **Credencial de acesso:** Uma credencial de acesso identifica a pessoa perante o sistema, podendo ser um crachá, uma digital, uma TAG etc.
- **Consumo de crédito:** O Consumo de crédito é um tipo de validação de acesso onde a pessoa deve possuir uma faixa de acesso vinculada a um crédito. A cada passagem pelo dispositivo em um horário determinado a quantidade de crédito é decrementada, o que se chama de consumir o crédito.
- **Concentradora:** Ver DFS.
- **Controle de nível:** O controle de nível indica se a pessoa pode ir de um nível origem para um nível destino. Para conseguir chegar no nível de destino a pessoa deve estar no nível de origem. **Exemplo:** Em um dispositivo que dá acesso do nível 1 para o nível 2, somente as pessoas que estão no nível 1 terão acesso válido para o nível 2.
- **CCTV:** Do inglês "closed-circuit television", é o mesmo que CFTV.
- **CENTRAL DE MONITORAÇÃO (em inglês: Centr:** Local especialmente projetado para recepção de sinais oriundos dos sistemas de alarme instalados remotamente, bem como execução dos serviços de monitoração e controle destes sinais, por plantonistas ou operadores. A palavra monitoramento, largamente utilizada, não se encontra na língua portuguesa, sendo apenas uma adaptação da palavra inglesa "monitoring". O dicionário Aurélio cita apenas as palavras monitoração e monitorização como corretas. (.....) Outros termos popularmente empregados:

Central de Monitoramento, Plantão de Monitoria, Plantão Operacional; Estação Monitora; etc.

- **CFTV:** Circuito Fechado de Televisão.
- **Comando predecessor:** Dependendo do comando enviado aos dispositivos é necessário que outro comando seja enviado e executado anteriormente para que a operação tenha êxito. Ex: comando: alterar data da leitora. Neste caso é necessário enviar um comando para bloquear o controlador da leitora, a hora é atualizada e posteriomente deve-se enivar um comando para desbloquear o controlador.
- **Comunicação síncrona:** É uma forma de troca de informações/mensagens entre emissor e receptor. Quando um envio é feito, o processo remetente é bloqueado até que a recepção correspondente seja realizada, ou seja, o transmissor/receptor não consegue encaminhar um nova mensagem enquanto a resposta não chega.
- **Comunicação assíncrona:** Em uma comunicação assíncrona, cada bloco de dados inclui um bloco de informação de controle (chamado flag), para que se saiba exatamente onde começa e acaba o bloco de dados e qual a sua posição na seqüência de informação transmitida. Nesse tipo de comunicação o receptor/transmissor pode encaminhar quantas mensagens ele quiser, desde que a mensagem anterior seja entregue, ele não necessita de uma resposta e sim da conclusão do envio da mensagem.
- **Corporate safety:** Relacionado a segurança do trabalho.
- **Corporate security:** Relacionado a segurança patrimonial.
- **Cofre coletor:** Dispositivo que obriga a devolução do crachá na saída de visitantes, terceiros ou de crachás provisórios. Após colocar o crachá no cofre coletor a pessoa não consegue mais pegar o crachá de volta. Somente abrindo o cofre com chave é possível coletar o crachá.
- **Comprovante:** Termo da Portaria 1510. É o comprovante de Registro de Ponto do Trabalhador e é um documento impresso para o colaborador acompanhar suas marcações diárias de ponto.
- **Controle de créditos de acesso:** Determina a quantidade de vezes que um crachá terá acesso num dispositivo, em uma determinada faixa horária. O controle de crédito de acesso exige que a pessoa possua créditos para acessar determinado dispositivo/leitora. Ao passar o crachá na leitora será verificado se i) a pessoa possui uma faixa de créditos; e, ii) se possui crédito para esta faixa.
- **Crachá desatualizado:** O crachá é considerado desatualizado quando a data da última atualização do mesmo, em comparação com a data atual, resultar uma quantidade de dias maior que o tempo de expiração de pendências.
- **ContPlanta:** O ContPlanta é um tipo de validação de data de validade de ASO e treinamento de segurança por planta. A validade do ASO e do treinamento de segurança pode ser diferente de planta para planta, isso porque uma planta pode oferecer mais riscos à saúde que outra, por exemplo. Neste caso sempre vai valer a menor data de validade que a pessoa possuir.
- **Database SID (Oracle):** Identificador utilizado para identificar unicamente uma base de dados específica dentro de um sistema. Por essa razão, um computador não pode ter mais do que um SID de mesmo nome configurado. Fonte: http://www.orafaq.com/wiki/ORACLE_SID.
- **Database instance (SQL Server):** Nome que representa um identificador único para uma instalação do MS SQL Server dentro de um computador.
- **Deadlock:** Deadlock é o termo utilizado para designar um erro que acontece quando duas sessões entram numa situação de conflito, cada qual aguardando pela liberação de bloqueios que a outra sessão mantém.
- **Deploy:** *Deploy* de software trata de todas as atividades que fazem um programa ficar disponível para uso (vulgarmente, "subir o programa"). A ação contrária é conhecida como *undeploy*, e serve para indisponibilizar (vulgarmente, "derrubar") uma aplicação.
- **Desistência de acesso:** Indica que uma pessoa que teve o acesso válido desistiu de acessar o local pretendido. A desistência de acesso somente é percebida em dispositivos que possuem catraca (catraca, torniquete, clip).
- **DFS:** Sigla para **Digicon Framework Server**, conjunto de rotinas e utilitários padronizados para facilitar o desenvolvimento da integração entre os dispositivos Digicon de Controle de Acesso e Ponto, este framework é o motor do Middleware nas aplicações de alto nível. O DFS é responsável pela comunicação com todos os dispositivos, componente de software de alto nível e/ou hardware da solução, permitindo a distribuição do processamento de comandos e eventos em vários servidores.

- **DHCP:** O protocolo DHCP (protocolo de configuração dinâmica de hosts) é um padrão IP que simplifica o gerenciamento da configuração IP do host. O padrão DHCP prepara o uso de servidores DHCP como uma forma de gerenciar a alocação dinâmica de endereços IP e outros detalhes de configuração relacionados para os clientes com DHCP da rede. Todos os computadores de uma rede TCP/IP devem ter um endereço IP exclusivo. O endereço IP (junto com a máscara de sub-rede relacionada) identifica o computador host e a sub-rede à qual ele está anexado. Quando você move um computador para uma sub-rede diferente, o endereço IP deve ser alterado. O DHCP permite que você atribua dinamicamente um endereço IP a um cliente a partir de um banco de dados de endereço IP de servidor DHCP na rede local.
- **Display:** Visor gráfico acoplado em alguns dispositivos de acesso, utilizado para escrever mensagens para o usuário.
- **Dispositivo controlador:** É o dispositivo principal gerenciado pelo sistema. A partir dele que controlamos os demais dispositivos (leitoras, sensores, saídas).
- **DLL:** Dynamic Link Library, biblioteca de vínculo dinâmico, desenvolvida inicialmente pela Microsoft para o conceito de biblioteca compartilhada.
- **DOME:** São as proteções para câmeras em forma de globo ou bolha (quando embutidas no teto, paredes ou cantos) que tem a função de camuflar em seu interior, protegendo e impedindo que seja visualizada a movimentação da câmera.
- **DVR (Digital Video Recorder):** Gravador de vídeo digital. Duas variações podem ser percebidas: Solução embarcada ou Solução baseada em um PC. A solução embarcada é um equipamento próprio com software embutido. A solução baseada em PC é normalmente uma placa de e um software de captura de imagens.
- **DXF:** O DXF AutoDesk Drawing Interchange format é um arquivo de intercâmbio para modelos de CAD. É reconhecido como uma espécie de padrão internacional para todos os programas de cad e áreas correlatas. O Mapa de Ambientes suporta oficialmente a importação desse tipo de arquivo nas versões do AutoCAD R12, 2000, 2004 e 2006. Outras versões são parcialmente suportadas.
- **Eletromagnetic Coupling:** Sistemas que usam um campo magnético como um meio de transferir dados ou energia.
- **Endereço IP:** É o endereço que identifica o dispositivo na rede.
- **Evento:** É a ocorrência de um alarme ou acesso.
- **Evento on-line:** É o evento que pode ser recebido e armazenado pela aplicação no momento de sua ocorrência, ou seja, todo os componentes da solução devem estar ativos e com a comunicação estabelecida. Caso contrário o evento será considerado off-line.
- **Entrada digital dependente:** Uma entrada digital dependente é uma entrada digital que participa da validação de acesso. Além da passagem do crachá ou biometria, uma entrada digital deve ser acionada ou desativada para que o acesso seja válido. Exemplo: Uma porta eclusa, onde o acesso só é permitido as duas postas estiverem fechadas. Além da validação do crachá o dispositivo deve receber um sinal pela entrada digital que de ambas as portas estão fechadas.
- **Entrada digital:** Entrada digital é uma entrada onde é lido um sinal de ligado ou desligado. As entradas digitais são geralmente utilizadas para ler sinais de alarmes.
- **Estado padrão de uma entrada digital:** É o valor inicial de uma entrada digital. Sempre que a entrada digital apresentar este valor será considerada desativada. Quando o sinal for diferente do estado padrão a entrada será considerada ativa ou alarmada.
- **Faixa de acesso da permissão:** Par de horário composto de horário inicial e horário final. Esta faixa horária determina um intervalo de tempo em que o acesso é permitido. Ex: 07:30 a 18:30 - Indica que o acesso pode ser feito a apartir das 07:30 até as 18:30, inclusive com os horários limite.
- **Faixa horária:** Conjunto de hora inicial e hora final onde a hora incial sempre será maior que a hora final. Os horários limites fazem parte da faixa horária, ou seja, uma faixa que vai das 10:00 h às 11:00 h, indica que começa a ser válida a partir das 10:00:00 h e continua válida até às 11:00:00 h, inclusive.
- **Função:** Uma função é uma funcionalidade programada no dispositivo e acionada ao pressionar uma tecla. A função digitada no teclado do dispositivo e enviada juntamente com o evento. Como padrão todo evento tem a função 0 (zero).
- **Facility Code:** Traduzindo é o código da planta. Este controle é muito utilizado em cartões de proximidade para evitar que um cartão tenha acesso em outras plantas que não sejam do cliente. Normalmente é possivel configurar por leitor os facilities code que o leitor deve liberar o acesso.

- **Faixa de Horário de acesso:** É a escala definida no cadastro da pessoa.
- **FAR:** False Acceptance Rate: taxa de falsos positivos, refere-se à probabilidade de um utilizador não autorizado ser aceite. Este parâmetro deverá ser ajustado para evitar a fraude nos sistemas biométricos.
- **FER:** Failure to Enroll Rate: taxa de falas de alistamento, refere-se aos utilizadores que são rejeitados no momento do registo devido à má qualidade da sua amostra.
- **Fora de repouso (Equipamento):** Fora de repouso representa uma situação do equipamento. Determinados equipamentos têm uma entrada digital sendo controlada para indicar quando o equipamento está fora do seu estado original/normal. Imagine uma porta de fecho magnetico onde há um sensor sendo controlado quando a porta está fechada. Se alguem passar o cartão para passar nessa porta e o sensor que indica que a porta está fechada estiver fora do estado normal quer dizer que esse foi um acesso fora do estado de repouso. Pois a porta controlada não estava fechada como deveria.
- **FRR:** False Rejection Rate: taxa de falsas rejeições, refere-se à probabilidade de um utilizador que está autorizado ser rejeitado no momento em que tenta aceder ao sistema. Se os utilizadores são rejeitados erroneamente com frequência, parecerá que o sistema não funciona correctamente e deverá ser revisto.
- **FTE:** Failure to Enroll: indica a probabilidade numérica de alguém não ser registado devido a uma falha no momento de criar um padrão.
- **Gerência de Riscos:** Autor: Mussi A função, dentro do contexto empresarial, que visa a proteção dos recursos humanos, materiais e financeiros da empresa, quer pela eliminação, redução ou financiamento dos riscos conforme seja economicamente viável. Fonte: Manual de Análise de Risco.
- **Handkey:** Tipo de validação biométrica que mede o tamanho e o formato da mão do indivíduo para verificação de sua identidade.
- **Handpunch:** Equipamento da empresa Recognition System que utiliza a tecnologia de handkey para identificação de indivíduos.
- **Half-Duplex:** Sistema de comunicação aonde os dados são transmitidos em ambas as direções, mas não ao mesmo tempo.
- **Hard Antipassback:** Faz o Bloqueio do acesso da pessoa.
- **Horário Flexível:** Indica que o colaborador pode trabalhar em qualquer horário, desde que cumpra sua jornada de trabalho.
- **Horário Móvel:** Indica que o colaborador tem mobilidade na jornada de trabalho, podendo entrar mais cedo para sair mais cedo. Exemplo: Horário padrão: 08:00 às 12:00 e 13:30 às 18:00 Horário praticado: 07:00 às 12:00 e 13:30 às 17:00.
- **Interjornada:** Quantidade de tempo de descanso obrigatório entre duas jornadas de trabalho de uma pessoa. A pessoa somente pode iniciar uma jornada se tiver um tempo mínimo de descanço desde o término de sua última jornada de trabalho.
- **Inductive Coupling:** São sistemas que usam a indução de corrente em um enrolamento como um meio de transferir dados ou energia.
- **ID do dispositivo:** É o identificador único do dispositivo cadastrado na aplicação Ronda Acesso. Na aplicação recebe o nome de código do dispositivo.
- **JasperReports:** Biblioteca em Java utilizada para gerar relatórios.
- **Java:** Linguagem de programação orientada a objeto, desenvolvida na década de 90 por uma equipe de programadores chefiada por James Gosling, na empresa Sun Microsystems.
- **J2EE:** Java Platform Enterprise Edition ou Java Edição Empresarial é uma plataforma de programação para servidores na linguagem de programação Java.
- **JMS:** Java Message Service (JMS) é uma API para linguagem de programação Java utilizada para troca de mensagens entre sistemas.
- **JVM:** Java Virtual Machine, responsável pela interpretação do código Java.
- **Leitora Ativa_Passiva:** Trata-se uma leitora que está conectada a estação do usuário podendo ser acessada tanto local como remotamente.
  Estados possíveis:
  - Leitora ativa: A leitora está cadastrada e liberada para uso pelo usuário logado
  - Leitora passiva: A leitora está cadastrada porém não está liberada para uso pelo usuário logado.
  O status da leitora esta diretamente ligado ao usuário.
  Um usuário pode ter apenas uma leitora ativa. A mesma leitora pode estar ativa para mais de um usuário.
- **Listas:** Informações que são armazenadas em um controlador de acesso para trabalhar em modo off-line. As listas são consultadas no caso de queda de

comunicação entre os coletores e a base de dados. Observe que as listas digitais possuem uma particularidade. Estas listas permitem que sejam criadas listas de inclusão, e exclusão além de possibilitar o limite para cada uma delas. O aplicativo carregado no coletor também precisa estar configurado para suportar as listas cadastradas.

- **Local de Passagem:** Local de entrada ou de saída de pessoas ou de veículos em uma área controlada. Uma área controlada pode ter mais de um local de passagem. Um local de passagem somente dá acesso a uma área controlada, e pode ser controlado por um ou mais bloqueios físicos.
- **Local Físico:** Refere-se a uma área (local) sobre o qual incide um controle de acesso. É compatível com o antigo conceito de ambiente controlado, e pode ser um site, portaria, zona, área, andar, planta, etc.
- **Log4j:** Biblioteca em Java para geração de logs, utilizada no SDK.
- **MCA:** Módulo Controlador de Acesso Digicon. É uma placa controladora de dispositivos Digicon. A placa MCA pode controlar terminais de porta e/ou acesso, catracas, torniquetes, cancelas e monitoramento de ambiente.
- **MCA-Net:** Módulo controlador de acesso Digicon. A placa MCA-Net é mais compacta que a placa MCA, tendo as mesmas funcionalidades. A placa MCA-Net pode controlar terminais de porta e/ou acesso e catracas com até duas leitoras.
- **Mapa:** É uma visualização gráfica de um Plano de Localização Física.
- **Mapa de localização física:** É a representação gráfica da planta da empresa, com os dispositivos físicos de acesso e segurança.
- **Mapa SmartCard:** O Mapa SmartCard define as informações que estarão contidas no cartão smart card. Além de definir quais informações, o mapa tem a função de indicar onde exatamente estão estas informações. O SmartCard Mifare é composto de 16 setores com 4 blocos cada. Cada bloco contém 16 bytes de armazenamento. Ao todo são 1024 bytes no cartão. Alguns blocos são usados especificamente para manter a chave de logon no setor. Portanto, o mapa smartcard contém todos os campos (rotinas do acesso) que estarão no cartão e a posição de cada campo no cartão.
- **MCBF:** Mean Ciclys Between Failures = Quantidade de ciclos entre falhas.
- **Microsoft Outlook:** Aplicativo destinado ao envio e recebimento de e-mails e gerenciamento de compromissos e tarefas.
- **Middleware:** Em informática é um mediador, composto de hardware e/ou software, comumente utilizado para mover ou transportar informações e dados entre programas de diferentes protocolos de comunicação e plataformas.
- **Modbus:** Protocolo aberto de comunicação entre dispositivos eletrônicos. Descreve um padrão de como trocar informações com esses dispositivos através de registradores e sinais. Usa tabelas/mapas de registradores e sinais, porém, cada dispositivos usa o mapa da maneira que precisa, portanto, cada dispositivo especifica como tratar os seus registradores.
- **Módulo Controlador:** O módulo controlador é um dispositivo conectado ao dispositivo controlador que faz a interface do dispositivo controlador até os dispositivos finais que são as leitoras, sensores, entradas.
- **Monitor SmartCard:** As pendências enviadas pelo sistema ao monitor são atualizadas automaticamente no cartão smartcard ao passar o cartão na leitora. Ex: ao alterar permissões de acesso a determinados colaboradores é enviado uma pendência para a alteração de permissão ao monitor smartcard. O colaborador ao passar o cartão na leitora terá sua permissão de acesso atualizada.
- **Mascaramento de alarmes:** Mascaramento de alarmes é um procedimento em que é informado um período de empo em que os alarmes ocorridos não devem ser considerados como alarmes.
- **MP 1.510:** Portaria do Ministério do Trabalho e Emprego (MTE) que disciplina o controle de ponto eletrônico (www.mte.gov.br/pontoeletronico/).
- **MTBF:** Mean Time Between Failures = Quantidade de tempo de uso do equipamento entre falhas.
- **MTE:** Sigla para Ministério do Trabalho.
- **MRP:** Termo da Portaria 1510. Significa "Memória de Registro de Ponto" ou "Memória de Registro Permanente" é a memória que contém todos os registros de ponto e não pode ser apagada ou alterada.
- **MT:** Termo da Portaria 1510. Significa "Memória de Trabalho" é a memória que possui todos os dados necessários à operação do REP, esta possuirá dados do empregado e do empregador conforme definido na portaria.

- **Notificação de dispositivo:** Notificação de dispositivo é o termo usado para quando o gerenciamento de dispositivos precisa notificar o mesmo de alguma situação. É um "aviso" para o dispositivo. Exemplo: para dispositivos Digicon que controlam Smart card e o cartão precisa ser atualizado, o Servidor faz uma notificação de pendência, "avisando" o dispositivo que quando ler aquele crachá ele precisa solicitar as pendências para o Servidor.
- **NSR:** Termo da Portaria 1510. Significa "Número Seqüencial de Registro", este é um número exclusivo que cada marcação do ponto possui.
- **Online_offline:** Define o nível de comunicação entre o dispositivo e a aplicação. Online indica que existe a comunicação e offline indica que não existe a comunicação.
- **OPC - OLE for Proccess Control:** OLE = Object-Linking and Embedding. Especificação de padrões abertos para automação industrial. OPC define especificações de comunicação entre dispositivos diversos.
- **Permissão de área restrita:** São permissões de acesso às áreas restritas para os Colaboradores, Visitantes, Outras Unidades e Alunos. As permissões são informadas especificamente para um elemento/dispositivo. Cada pessoa pode ter até 3 permissões de áreas restritas. As permissões de áreas restritas são também chamadas de permissões adicionais.
- **Permissões adicionais:** Ver Permissão de área restrita.
- **Painel de Alarme (Alarm Pannel):** Equipamento que gerencia e controla sensores, sirenes, dispositivos de saída, teclados digitais, módulos de expansão, módulos receptores de sinais (rádio), comunicador telefônico (que pode já estar incorporado na mesma placa). (.....) Outros termos popularmente empregados: Central de Alarme; Terminal de Alarme; Placa de Alarme; Central Remota; Terminal Inteligente; Sistema de Alarme; etc.
- **Pendências:** São informações geradas automaticamente por processos do sistema, ou manualmente forçando atualização, as quais são enviadas para o smartcard para atualização das informações no cartão. Ex: baixa de histórico de crachá, baixa de crachá de visitantes, troca de permissão, crachá extraviado, etc.
- **PIN:** PIN - Personal Identification Number. Número que serve para identificar uma pessoa. Há sistemas de controle de acesso que permitem um acesso identificado sem cartão, nesse caso, em vez de digitar o número do cartão, é digitado o PIN. Há outras soluções que permitem acesso sem cartão, mas o valor digitado é o próprio número do cartão.
- **Plano de Localização Física (PLF):** É a representação hierárquica dos locais físicos de uma organização, podendo abranger localizações geográficas e prediais.
- **PLF:** Plano de Localização Física.
- **Porta Serial:** É o nome da porta onde está conectado o dispositivo.
- **Pré-Cadastro de Crachás:** O pré-cadastro de crachás é necessário quando não se utiliza uma forma definida para reconhecimento dos números do crachá, como Identificador ou Faixa. Neste, caso todos os crachás devem ser pré-cadastrados indicando a sua utilização. Também é utilizado para evitar que crachás desconhecidos sejam utilizados, pois apenas os crachás pré-cadastrados no sistema podem ser usados.
- **PTZ (Pan_Tilt_Zoom) - Câmeras:** Este recurso significa funções de "pan" (giro no plano horizontal), "tilt" (giro no plano vertical) e lente "zoom". Normalmente estas câmeras PTZ estão protegidas/camufladas por uma Dome.
- **Pictograma:** Sinalização luminosa que serve para indicar uma informação ao usuário.
- **Porta Fiscal:** Termo da Portaria 1510. A Porta Fiscal é uma porta USB externa que o dispositivo REP possui e é utilizada exclusivamente para captura dos dados armazenados na MRP pelo Auditor-Fiscal do Trabalho.
- **Programa de Tratamento de Registro de Ponto:** Termo da Portaria 1510. O "Programa de Tratamento de Registro de Ponto" é um conjunto de rotinas informatizadas que tem por função tratar os dados relativos à marcação dos horários de entrada e saída, originários exclusivamente do AFD, gerando o relatório "Espelho de Ponto Eletrônico", o Arquivo Fonte de Dados Tratados - AFDT e Arquivo de Controle de Jornada para Efeitos Fiscais - ACJEF.
- **Portaria 1510:** Esta é a portaria que disciplina o registro eletrônico de ponto e a utilização do Sistema de Registro Eletrônico de Ponto - SREP.

- **Porta Eclusa:** Controle feito entre duas portas que impede que as duas sejam abertas ao mesmo tempo. É um recurso utilizado em locais físicos que necessitam de um nível maior de segurança. O controle de porta eclusa é feito através de entradas digitais dependentes.
- **Quadro sinótico:** Quadro resumido.
- **RFID:** Tecnologia de Identificação por Radiofreqüência. É usada nas etiquetas inteligentes. RFID é uma tecnologia para identificar, rastrear e gerenciar uma enorme gama de produtos, documentos, animais e indivíduos, sem contato e sem a necessidade de um campo visual.
- **RCP:** Rich Client Platform – bilbioteca java baseada no SWT que oferece a possibilidade de construir interfaces mais ricas em recursos.
- **REP:** Registrador Eletrônico de Ponto, equipamento com característica própria desenhado para atender a Portaria 1.510.
- **Reset Antipassback:** É configurado um tempo para resetar o ultimo acesso da pessoa e permitir que seu próximos acesso seja permitido.
- **RF_AIS:** Sistemas Automáticos de Identificação por Rádio Freqüência.
- **RF_DC:** Sistemas de comunicação através de rádio entre um computador e um coletor.
- **RH:** Recursos Humanos.
- **Risco:** Uma ou mais condições de variáveis com potencial necessário de causar dano ao patrimônio da empresa, seja ele tangível ou intangível. Fonte: Manual de Análise de Risco.
- **RMI:** Invocação Remota de Métodos Tem o intuito de prover necessidades da tecnologia Java, para uma plataforma de objetos distribuídos.
- **RS-485:** RS-485 é uma versão atualizada do RS-422 e suporta até 32 dispositivos numa mesma conexão. RS-485 é uma especificação elétrica de 2 fios, half-duplex com conexão serial múltipla. Ele permite implementar redes com baixo custo e oferece alta velocidade de comunicação (10Mbit/s) e suporta relativamente grandes distancias (1200 metros). RS-485 especifica somente características elétricas do driver e do receiver, ele não define ou especifica o protocolo de comunicação.
- **Reações automáticas:** É quando um dispositivo envia comandos para outros dispositivos. Ex: ao passar o crachá numa leitora esta envia um comando para a porta abrir ou não, conforme as permissões de acesso da pessoa.
- **RTC:** Real Time Clock - É o relógio do processador do sistema operacional. Determina a data e hora que o sistema operacional utiliza em seus processos.
- **Reconhecimento da digital:** Processo que utiliza a impressão digital de uma pessoa para efetuar o seu reconhecimento. A impressão digital da pessoa é capturada e analisada, de onde são extraídos pontos que fornecem uma identificação.
- **REP:** Registrador Eletrônico de Ponto. Equipamento inviolável, com capacidade para emitir documentos fiscais e realizar controles de natureza fiscal, referentes à entrada e à saída de empregados nos locais de trabalho. O fabricante do REP deverá ser cadastrado no MTE e está obrigado a registrar cada um dos modelos produzidos, apresentando um "Certificado de Conformidade do REP à Legislação" emitido por órgão técnico credenciado e a fornecer, tanto para o MTE como para o cliente empregador, um "Atestado Técnico e Termo de Responsabilidade". Fonte: http://www.administradores.com.br/informe-se/informativo/o-novo-registro-eletronico-do-ponto-de-empregados/25813/.
- **Reconhecimento de alarme:** O reconhecimento de um evento de alarme é o modo que o operador de segurança possui de indicar ao sistema que está ciente de uma ocorrência dentro da empresa.
- **Revista aleatória:** A revista aleatória é um recurso que permite que o dispositivo sorteie de modo aleatório algumas pessoas que passam pelo mesmo, para que sejam submetidas a uma revista. O objetivo da revista é principalmente o desencorajamento da prática de furtos.
- **Smart Card as proximity:** Indica que o crachá Smart Card é utilizado como se fosse um cartão de proximidade. A validação de acesso é feita apenas com base no número físico do crachá. É recomendado quando utilizam-se cartões compartilhados com outras empresas. Exemplo: Usar o cartão de transporte de ônibus para efetuar o acesso.

- **SAD:** Controle utilizado pela Petrobrás para definir suas plantas físicas. Cada SAD corresponde a uma unidade física. No sistema Ronda Acesso, o SAD corresponde a Filial.
- **SDK:** Software Development Kit, ou seja, Kit de Desenvolvimento de Software, pacote que inclui ferramentas (APIs, linguagens de scripting e interface gráfica de usuário) necessário para que desenvolvedores de software implementem aplicações que complementam um sistema original, adicionando valor a este sistema.
- **Senha_Contra-senha (password):** Pergunta (senha) e resposta (contra-senha) utilizadas para a confirmação ou não sobre a veracidade de um disparo de alarme ou pânico, as quais somente os usuários do sistema de alarme remotamente instalado e os operadores da Central de Monitoração devem conhecer. Algumas empresas preferem trabalhar identificando-se normalmente para o cliente e esperando apenas uma palavra de confirmação ou não (palavra-chave). (.....) Outros termos popularmente empregados: Pergunta Chave / Resposta Chave; Palavra Chave; etc.
- **Sensor:** Um dispositivo que responde a um estímulo físico e produz um sinal eletrônico.
- **Sensor Dupla Tecnologia:** Componente do sistema, que detecta o movimento do intruso em um ambiente internamente protegido pelo sistema de alarme. Seu funcionamento baseia-se em duas tecnologias de detecção: através do processo de Infravermelho Passivo e Microondas. (.....) Outros termos popularmente empregados: Sensor Conjugado; Sensor Dual Safe; Sensor Microondas; Sensor de Presença, Sensor de Movimento, Sensor Volumétrico, etc.
- **Sensor Infravermelho Passivo:** Componente do sistema, que detecta o movimento do intruso em um ambiente internamente protegido pelo sistema de alarme. Seu funcionamento baseia-se na detecção da aproximação e afastamento de uma fonte calórica (a qual emite raios infravermelhos) (.....) Outros termos popularmente empregados: Sensor de Presença; Sensor IVP; Sensor PIR; Sensor de Movimento, Sensor Volumétrico, etc.
- **Serviço:** É um processo que inclui programações automáticas que serão startadas assim que o serviço é inicializado, não dependendo de uma pessoa para cadastrar as programações.
- **Serviço de Pronta Resposta:** Refere-se ao serviço de pronto atendimento em casos de disparo de alarme no sistema de alarme instalado remotamente, no intuito de se verificar a veracidade do sinal recebido na central de monitoração, antes de se comunicar à polícia, para socorro. O pessoal e o veículo são enviados ao local tem a função de apoio ao cliente, meramente técnico e informativo, através da verificação externa do local e comunicação por rádios e telefones celulares, não lhes cabendo o combate ou repressão à marginalidade. (.....) Outros termos popularmente empregados: Apoio Local; Apoio Tático; Apoio Técnico; Verificação Local; Unidades Volantes de Atendimento; Unidades de Apoio Móvel; Viatura de Verificação Externa; etc.
- **Site:** Pode ser definido como uma localização física de uma empresa e que possui algum gerenciamento de controle de acesso e segurança (ambiente monitorado).
- **Snap:** Funcionalidade que cria pontos pré-definidos, porém invisíveis na visualização gráfica, com o objetivo de facilitar a edição de elementos na planta. Esse recurso força as ferramentas (como a de criação de linhas) a funcionarem somente sobre esses pontos pré-definidos, garantindo a possibilidade de se criar desenhos simétricos e com ângulos retos. Disponível no Editor de Ambientes, o recurso pode ser ativado e desativado de acordo com a preferência do usuário.
- **SOAP:** Simple Object Access Protocol, base para construção de WebService.
- **Soft antipassback:** Permite a passagem da pessoa mas gera um evento de violação do antipassback para o monitoramento e para registro.
- **Solenóide:** Fio metálico enrolado em hélice sobre si mesmo (como eixo) que toma as propriedades do íman quando percorrido por uma corrente elétrica.
- **Sagem:** Fabricante de sensor biométrico amplamente utilizado entre os fabricantes de dispositivos de controle de acesso e ponto.
- **Sensor de Tamper:** O sensor de tamper é um sensor que indica se um dispositivo foi aberto ou fechado. Este tipo de sensor é utilizado para detectar violações em dispositivos de acesso e ponto.
- **SIT:** Termo da Portaria 1510. Sigla para "Secretaria de Inspeção do Trabalho". É a secretaria lotada no MTE que define os parâmetros e os cadastros previstos na Portaria 1510.

- **SREP:** Termo da Portaria 1510. Sistema de Registro Eletrônico de Ponto ou SREP, é o conjunto de equipamentos e programas informatizados destinado à anotação por meio eletrônico da entrada e saída dos trabalhadores das empresas, previsto no art. 74 da Consolidação das Leis do Trabalho - CLT e aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.
- **SSL:** SSL (Secure Sockets Layer) é uma tecnologia de segurança que é utilizada para codificar os dados transferidos entre o computador de um utilizador e um servidor. O protocolo SSL, através de um processo de encriptação dos dados, previne que os dados transmitidos possam ser interceptados, ou mesmo alterados no seu percurso entre o navegador (browser) do utilizador e o servidor com o qual ele está ligado, garantindo desta forma a troca de informações confidenciais, como os dados de cartão de crédito ou informações pessoais de usuários.
- **Tag:** O transmissor/receptor mais o mecanismo de armazenamento de informações (chip + antena).
- **Tolerância de interjornada:** Indica a quantidade de tempo que uma pessoa pode retornar à sua jornada de trabalho sem que se caracterize que foi iniciada uma nova jornada de trabalho.
- **Tipo de função:** O tipo de função é a funcionalidade associada à uma tecla do dispositivo. Existe no sistema tipos de função para cadastrar biometria, digitar número do cadastro, ignorar nível, reservar e cancelar refeição, etc. Assim, cada tecla do dispositivo pode ser associada a um tipo de função. Por exemplo, a tecla 5 pode reservar refeição e a tecla 6 cancelar. Neste caso a função é 5 ou 6 e o tipo de função é reservar e cancelar refeição.
- **Template biométrico:** Atributos únicos extraídos das características biométricas de uma pessoa e convertidos em um código matemático. Um template pode ser extraído de uma digital, uma íris, de uma mão, etc.
- **Tags ativos (Active Tags):** São transponders que usam bateria como fonte de energia.
- **Tags passivos (Passive Tags):** Tags passivos não contém nenhuma fonte de alimentação interna. Eles são alimentados pelo próprio leitor.
- **Tagsys:** Etiqueta de identificação por radiofrequência. Etiquetas ou cartões inteligentes.
- **Turnstiles:** Catracas.
- **Timeout:** Tempo máximo de execução de um processo. O timeout define quanto tempo um processo pode esperar por determinada execução.

- **Tratamento de alarme:** O tratamento de um evento de alarme é o modo que o operador de segurança possui de indicar ao sistema que uma ocorrência de alarme está resolvida ou, pelo menos, recebeu algum tipo de atenção. Ao tratar um evento, um registro da ação é armazenado dentro do sistema para consultas futuras. O sistema permite que um alarme seja tratado automaticamente, ao receber um segundo alarme do mesmo tipo indicando a normalização da situação.
- **TNS Names:** TNSNAMES é um arquivo de configuração que define os endereços das bases de dados para que se possa estabelecer conexões com elas. O arquivo normalmente reside no diretório [ORACLE HOME]\NETWORK\ADMIN. Fonte: http://www.orafaq.com/wiki/Tnsnames.ora.
- **Tempo de expiração de pendência:** É o tempo que uma pendência aguarda para ser atualizada no Smart Card. Caso passe este tempo e a pendência não foi atualizada a mesma será descartada. Esta propriedade do sistema deve ser informada em quantidade de dias.
- **UTC:** *Universal Time Coordinated* ou Tempo Universal Coordenado é o fuso horário de referência a partir do qual se calculam todas as outras zonas horárias do mundo (fusos hrários). É o sucessor do Tempo Médio de Greenwich (Greenwich Mean Time), abreviadamente GMT. A nova denominação foi cunhada para eliminar a inclusão de uma localização específica num padrão internacional.
- **UTC-0:** UTC utilizado como base para determinação dos demais fusos horários.
- **UMBRAL:** é um tipo de referência, é a pontuação que determina a consistência de um padrão. Esta pode ser ajustada dependendo do nível de segurança.
- **Uso da marcação:** O uso da marcação indica para que ela serve ou para que ela foi utilizada dentro do sistema Ronda Acesso e Segurança. É uma lista pré-cadastrada com itens como "acesso", "marcação de ponto", "marcação de refeitório", entre outros.

- **Validação 1:1:** Conferência feita para saber se a pessoa que apresenta a biometria é a pessoa que diz ser. A biometria apresentada é comparada com a biometria de uma pessoa já identificada.
- **Validação 1:N:** Conferência feita para identificar uma pessoa em uma coleção de templates biométricos. A biometria apresentada é comparada com uma coleção de templates com o objetivo de identificar quem é a pessoa.
- **Visão Lógica:** É a visão gráfica dos dispositivos e suas respectivas conexões independentemente da localização física dos mesmos.
- **Validade do ASO:** A validade do ASO é a validade do Atestado de Saúde Ocupacional.
- **Validade de treinamento de segurança:** Alguns ambientes somente podem ser acessados após a pessoa passar por um treinamento. Para alguns ambientes, em geral de maior risco, este treinamento deve ser renovado periodicamente. O período em que o treinamento deve ser renovado é que se dá o nome de validade de treinamento de segurança.
- **Windows:** Marca registrada de sistema operacional da Microsoft Corporation. (www.microsoft.com).
- **WorkFlow:** Aplicativo usado para o controle e monitoramento das tarefas.
- **Webservice:** Web service é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes.
- **WSDL:** Web Services Description Language, linguagem para Desenvolvimento e descrição de WebService.