COMUNICAÇÃO E SEGURANÇA

MA 300

Guia do Usuário

Sumário

1 Apresentação

O **MA 300** da CS é um controle de acesso biométrico e proximidade RFID que possui um elevado desempenho. Seu avançado algoritmo proporciona velocidade e precisão nas leituras. Seu gabinete metálico com grau de proteção IP65 possibilita sua aplicação em condições adversas. O **MA 300** oferece ainda a versatilidade do uso autônomo ou gerenciado por software. Quando funcionando de forma autônoma o administrador pode utilizar um cartão ou teclado externo para realizar as configurações.

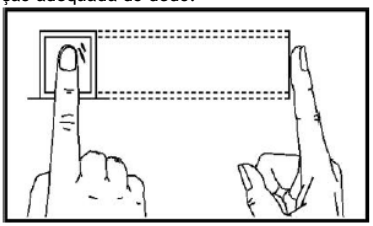
2 Instrução de Uso

2.1 Posição do Dedo

Dedos recomendados: O dedo indicador, dedo médio ou o dedo anelar.

Dedos não recomendados: O polegar e o dedo mínimo (por serem comumente difíceis de coletar a impressão digital na tela).

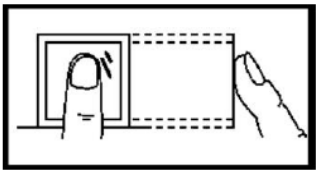
1. Posição adequada do dedo:



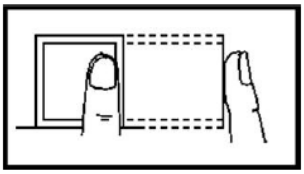
O dedo está ajustado à superfície e centralizado na guia

2. Posição inadequada do dedo:

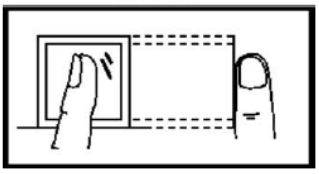
Não ajustado à superfície



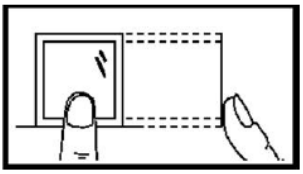
Fora do centro



Inclinado



Fora do centro



Integrado com um módulo de leitura de cartão RF, este dispositivo suporta o cartões de ID 125kHz. Por oferecer múltiplos modos de verificação tais como a verificação de impressão digital e verificação de cartão RF, este dispositivo pode se acomodar para diversas necessidades dos usuários.

Faça a leitura dos cartões na área do sensor seguindo a instrução de comando de voz e remova seu cartão após o dispositivo realizar a leitura.

Precauções

Proteja o dispositivo da exposição direta à luz solar ou a raios fortes, considerando que estes afetam consideravelmente a coleta da impressão digital e leva à falha na verificação da impressão digital.

Recomenda-se que o dispositivo seja usado sob temperatura de 0 - 50°C de modo a se alcançar um ótimo desempenho. Em caso de exposição do dispositivo a áreas externas por longos períodos de tempo, recomenda-se a adoção de bloqueadores de sol e instalações de dissipação de calor porque temperaturas excessivamente altas ou baixas podem diminuir a operação do dispositivo e resultar em altas taxas de rejeição falsa (FRR) e taxa de aceitação falsa (FAR).

Ao instalar o dispositivo de controle de acesso, favor conectar o cabo de força depois de conectar os outros cabos. Se o dispositivo não funcionar adequadamente, certifique-se de desligar o fornecimento de energia antes de executar a inspeção necessária. Note que qualquer trabalho com linha viva pode causar danos ao dispositivo, anulando assim os termos de garantia deste produto.

Para questões que não são cobertas neste documento, favor recorrer aos materiais relacionados incluindo o Guia de Instalação do Dispositivo, Manual do Usuário do Software de Gerenciamento de Controle de Acesso.

3 Introdução ao Dispositivo de Controle de Acesso

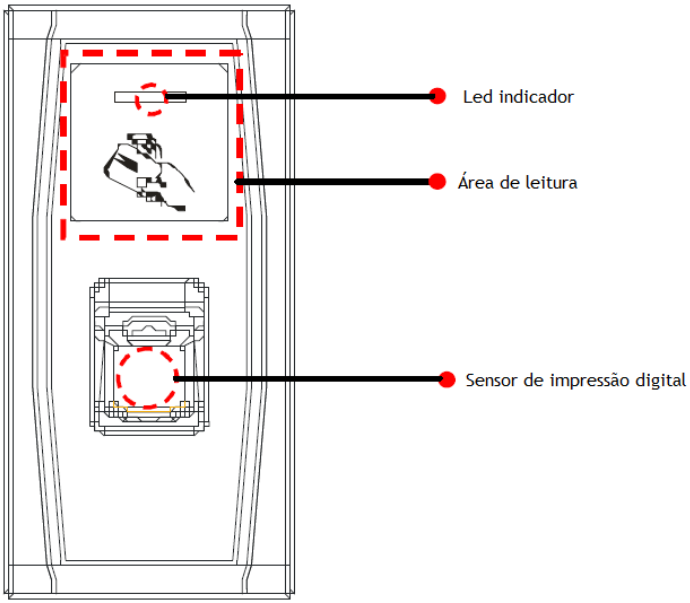
3.1 Visão Geral das Funções do Dispositivo

Como dispositivo de integração de controle de acesso e impressão digital, nosso produto pode ser conectado com uma trava eletrônica ou um controlador de acesso. Este dispositivo inclui operações simples e flexíveis e suporta o uso de cartões de gerenciamentos. Com um cartão de gerenciamento, podem-se desempenhar funções tais como registro off-line, registro de usuário e gerenciamento de pendrive. O comando de voz servirá de guia em todos os processos operacionais sem mostrador de tela. Este dispositivo vem sem teclado, mas permite a conexão com um teclado externo e oferece múltiplos modos de operação. Suporta múltiplos modos de comunicação. As características do pendrive incluem operações simples e convenientes. O design à prova de água e o revestimento de metal do dispositivo permitem que este resista a fortes impactos sem sofrer danos.

Incluindo um projeto compacto e simples, este dispositivo permite aos usuários conectar vários dispositivos através de um PC e realizar o monitoramento em tempo real.

3.2 Aparência do Produto

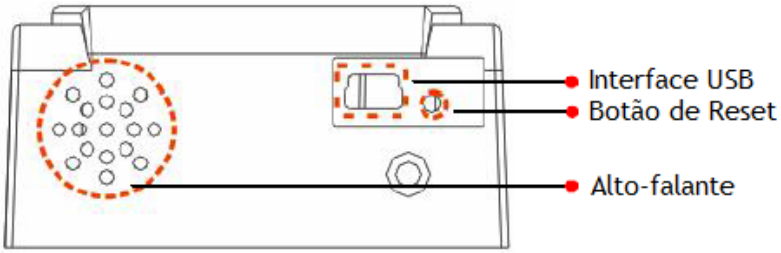
Vista Frontal:



- **LED indicador:** O LED indicador é usado para mostrar os resultados de operação do dispositivo e condições excepcionais que são definidas a seguir:
- **Regras comuns:** Se uma operação for bem-sucedida, o LED indicador verde acende por um segundo, caso contrário, o LED indicador vermelho acende por um segundo.
- **Estado de registro:** O LED verde pisca três vezes a cada três segundos.
- **Exclusão de usuário simples:** O LED vermelho pisca três vezes a cada três segundos.
- **Estado de verificação:** O LED verde pisca uma vez a cada dois segundos.

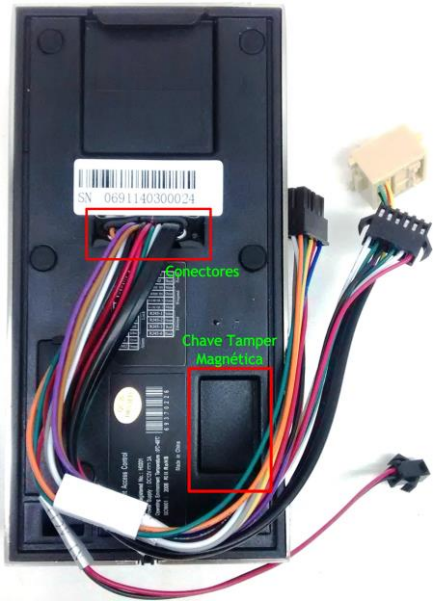
Área de leitura: refere-se à área quadrada com linha vermelha pontilhada, conforme mostrado na figura acima.

Sensor de impressão digital: Usado para coletar e combinar impressões digitais e para apagar usuários. Vista inferior:



- **Interface USB**: Usada para conectar com um pen drive ou um teclado.
- **Botão Reset:** Usado para reiniciar o dispositivo.
- **Alto-falante:** usado para reproduzir o som de bipe e o comando de voz. Se um usuário passar na identificação, o alto-falante bipa uma vez ; se o usuário não passar na verificação, o alto-falante emite um bipe curto e um bipe longo. Os padrões durante operação: bipe + comando de voz.

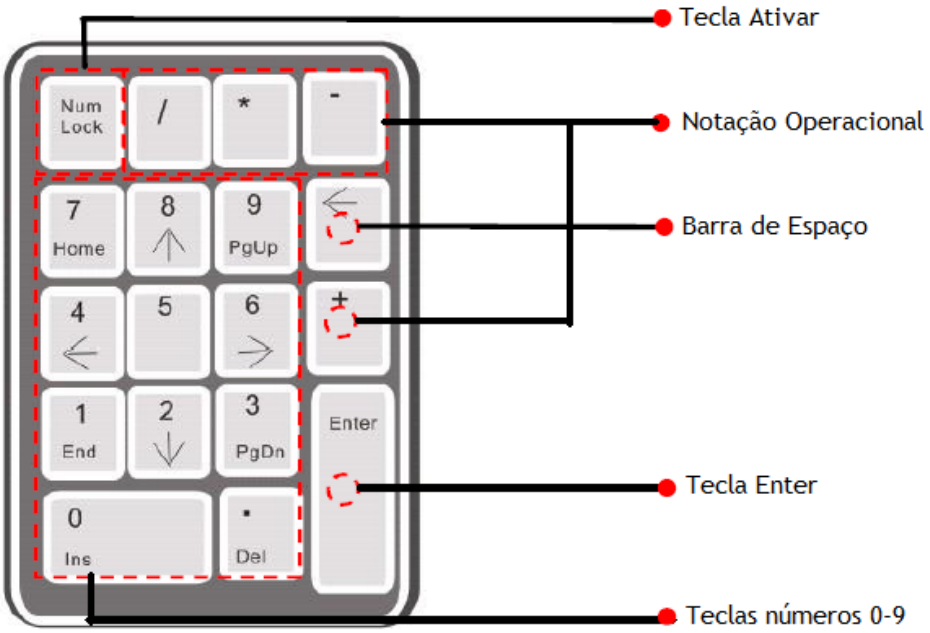
Vista Traseira:



- **Bornes: conexões com as travas e alimentação entre os cabos.**
- **Interface TCP/IP:** A interface TCP/IP conecta um PC por meio de um cabo de rede (para uma conexão detalhada, ver o Guia de Instalação).
- **Chave Tamper**: usado para gerar um alarme de segurança. Para detalhes, ver 3.5 Chave Tamper.
- **DIP Switch:** O DIP Switch possui quatro pinos numerados 1, 2, 3 e 4. No modo de comunicação RS485, os primeiros pinos 1, 2 e 3 são usados para ajustar o número do dispositivo de hardware e o quarto pino é usado para selecionar a condição aberta/fechada da resistência terminal. Para configurações detalhadas, ver o Guia de Instalação.

3.3 Uso de um Teclado USB Externo

Para facilitar as operações do dispositivo, pode-se conectar o dispositivo com um teclado USB externo (adquirido pelo usuário) e convenientemente realizar operações como registro de usuário, apagar e restaurar configurações de fábrica, especialmente quando se classifica IDs de usuário durante registro e exclusão de usuário.



Um teclado USB externo é mostrado acima:

NumLock é um teclado numérico. É ativado por configuração padrão. Se estiver ativado, o LED indicador ficará aceso. Quando o dispositivo está conectado com um teclado externo, podem-se usar somente as teclas numéricas, barra de espaço e a tecla Enter no modo NumLock ativado.

3.4 Estado de Verificação

Estado de Verificação: Após ligar o dispositivo, o mesmo inicia o estado de verificação caso você tenha registrado ou quando registrar com sucesso um cartão de gerenciamento ou em caso de encerramento de alguma operação.

No estado de verificação, todos os usuários possuem permissão para verificar suas identidades e desbloqueá-las (o administrador que possuir um cartão de gerenciamento somente pode desbloquear usando suas impressões digitais previamente registradas); o administrador pode realizar operações como registro/exclusão de usuário, gerenciamento de pen drive e operações com teclado.

3.5 Cartão de Gerenciamento

Os usuários do dispositivo são classificados como administrador ou usuários comuns.

Administradores: Um administrador tem permissão para realizar todas as operações incluindo registro/exclusão de usuário (exclusão de todos os outros usuários exceto ele mesmo) e gerenciamento de pen drive. Os privilégios dos administradores do dispositivo são implementados através dos cartões de gerenciamento.

Usuários comuns: usuários comuns somente têm permissão para verificar sua própria identidade e desbloquear. Um cartão de gerenciamento é um cartão especialmente alocado para um **super administrador**. Cada dispositivo deve registrar pelo menos um cartão de gerenciamento. Se nenhum cartão de gerenciamento estiver registrado, nenhuma operação poderá ser realizada e o sistema irá gerar uma mensagem de voz: "Please register the management card" (Favor registrar o cartão de gerenciamento).

Você pode implementar diferentes funções de acordo com as vezes que o cartão de gerenciamento for lido:

Nenhum pen drive e teclado externo estão conectados:

Ao ler o cartão de gerenciamento uma vez, pode-se acessar o estado de registro de usuário único.

Ao ler o cartão de gerenciamento cinco vezes consecutivas, pode-se entrar no estado de exclusão de usuário único.

Pen drive está conectado:

Ao ler o cartão de gerenciamento uma vez, pode-se entrar no estado de gerenciamento do pen drive.

Um teclado externo está conectado:

Ao ler o cartão de gerenciamento uma vez, pode-se ativar o teclado externo.

Leituras consecutivas: significa o intervalo entre duas leituras seguidas em menos de 5 segundos.

Os cartões de gerenciamento podem ser excluídos por meio da função "Limpar Tudo" do teclado, ou ter seus privilégios de administrador apagados por meio de software antes de serem excluídos como cartões de ID comuns. Para detalhes, ver Instruções Operacionais do Software de Controle de Acesso.

As impressões digitais do usuário portador de um cartão de gerenciamento só podem ser registradas por meio de software. Para detalhes, ver Instruções Operacionais do Software de Controle de Acesso.

Dica: Usuários que portarem cartões de gerenciamento só podem verificar suas identidades e desbloquear usando suas impressões digitais previamente registradas.

3.6 Senha do Sistema

Uma senha de sistema é uma senha usada para aumentar a segurança dos dados do dispositivo em comunicações TCP/IP ou RS485.

Dica: A senha do sistema pode ser modificada por meio do software de controle de acesso. Para detalhes, ver Instruções Operacionais do Software de Controle de Acesso.

3.7 Tempo Limite de Operação

O tempo limite de operação padrão é de 30 segundos. Quando se registra um cartão de gerenciamento ou exclui/registra um usuário (incluindo o registro com teclado externo e estados de exclusão de usuário), o sistema automaticamente faz solicitação a cada 10 segundos se não houver operação e retorna ao estado de verificação após fazer solicitação três vezes. A mensagem gerada é: "*Operation timeout. The system returns to verification state*". (Tempo Limite de Operação. O sistema retornará ao estado de verificação).

Dica: pode-se configurar o tempo limite por meio do software de controle de acesso.

4 Operações do Dispositivo

4.1 Cartão de gerenciamento

4.1.1 Cartão de gerenciamento de registro

Para registrar um cartão de gerenciamento, proceda da seguinte forma:

1. O dispositivo detecta automaticamente se existe um cartão de gerenciamento.

2. Se o dispositivo falhar em detectar a presença de um cartão de gerenciamento, ele entra no estado de registro de cartão de gerenciamento. Então proceda com o passo 3; caso contrário, vá para o passo 5.

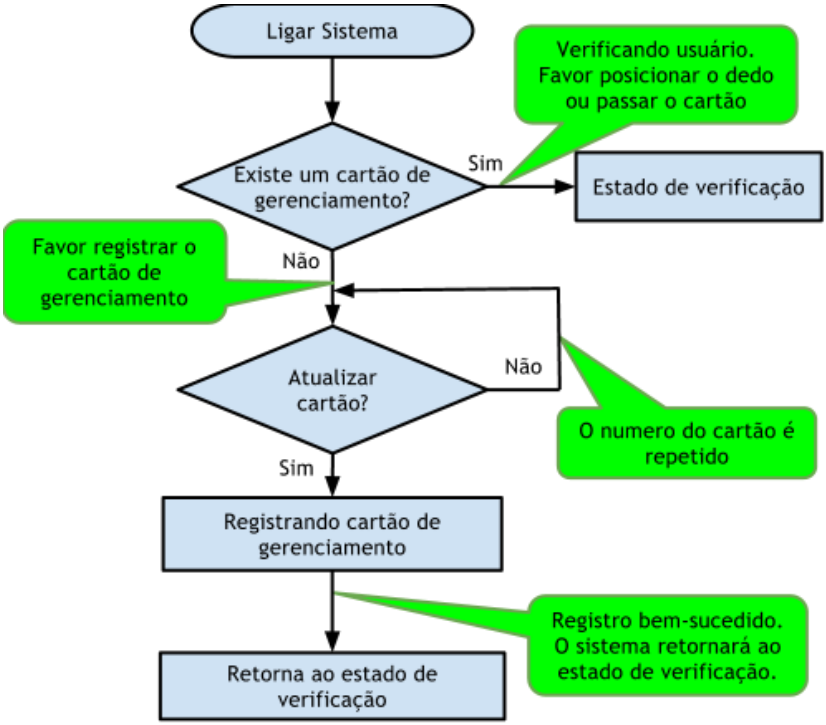
3. Após o sistema gerar a mensagem de voz : "*Please register the management card*". (Favor registrar o cartão de gerenciamento), pode-se fazer a leitura do cartão na área do sensor.

4. Se o registro falhar, o sistema gera a seguinte mensagem de voz: "*The card number is repeated* " (O número do cartão é repetido) e retorna ao passo 3; se o registro for bem-sucedido, o sistema gera a solicitação de voz: "*Registration is successfull. The system returns to verification state*" (Registro bem-sucedido. O sistema retornará ao estado de verificação).

5. Após retornar ao estado de verificação, o sistema gera a solicitação de voz: "*Verify users. Please press your finger or punch your card*". (Verificar usuários. Favor colocar o dedo ou passar o cartão).

Dica: o sistema retorna ao estado de verificação se qualquer operação atinge o tempo limite no passo 3 e somente solicita registro do cartão de gerenciamento novamente após o dispositivo ser religado.

Fluxograma do registro do cartão de gerenciamento é mostrado abaixo:



4.1.2 Registro de Usuário Comum

Registrar Cartão ID

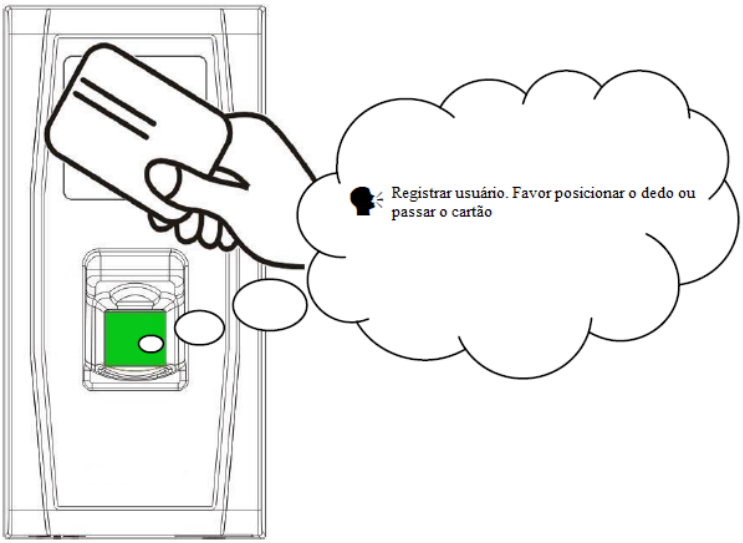
O modo para se entrar no estado de registro usando o cartão de gerenciamento é conhecido como o modo de registro do cartão de gerenciamento. Neste modo, pode-se registrar apenas um usuário. Quando se registra um novo usuário, o sistema designa automaticamente um ID ocioso ao usuário. Adicionalmente, pode-se também usar o modo de registro com teclado externo (para detalhes, ver 3.2.2 Registrar um Usuário por Meio do Teclado) para implementar registro de usuário com ID.

Em ambos os casos destes dois modos de registro, pode-se registrar novos usuários. Cada usuário tem permissão para registrar 10 impressões digitais e um cartão ID no máximo.

Para registrar um usuário, proceda assim:

1. No estado de verificação, o sistema vai para o estado de registro de usuário comum após a realização da leitura de cartão de gerenciamento uma vez. (No estado de registro, realizar a leitura de um cartão de gerenciamento uma vez fará retornar ao estado de verificação).

2. Após o sistema gerar a seguinte mensagem de voz: "*Register users. Please press your finger or swipe your card*" (Registrar usuários. Favor colocar o dedo ou passar cartão) pode-se iniciar o registro de usuário. Há os dois casos seguintes:



(1) Passar cartão ID pela primeira vez:

a. Quando se passa o cartão de ID novo e há sucesso no registro de um usuário, o dispositivo irá gerar a seguinte mensagem de voz: "*User number* **. *Registration is succesfull!*". (Número de usuário **. Registro foi bem-sucedido!). (** Refere-se à ID automaticamente designada ao usuário pelo sistema; mesmo que abaixo) e você pode proceder para o passo b; se o registro de usuário falhar, o sistema emitirá uma mensagem de voz: "*The card number is repeated*". (O número do cartão é repetido) e retorna ao estado de registro, aguardando a colocação do dedo ou a leitura do cartão.

b. Após o dispositivo gerar a seguinte mensagem de voz: "*Register. Please press your finger*" (Registrar. Favor pressionar dedo), o sistema entra no estado de registro de impressão digital especificado. Coloque o mesmo dedo novamente sobre o sensor três vezes seguindo a solicitação de voz.

c. Se o registro de impressão digital for bem-sucedido, o sistema irá gerar a mensagem de voz: "*Registration is successful. Register. Please press your finger*" (Registro bem-sucedido. Registrar. Favor colocar o dedo) e entra diretamente no próximo estado de registro de impressão digital; se o registro de impressão digital falhar, o sistema irá gerar uma mensagem de voz: "*Please press your finger again*" (Favor pressionar o dedo novamente) e repete o passo b.

d. o sistema retorna automaticamente ao estado de verificação quando os 10 dedos e o cartão ID são registrados, o cartão de gerenciamento é lido uma vez ou quando se atinge o tempo limite de operação.

(2) Coloque o(s) dedo(s) primeiro:

a. Coloque o mesmo dedo sobre o sensor três vezes, seguindo as solicitações de voz, seguindo a colocação adequada de impressão digital. Se o registro de impressão digital for bem-sucedido, o sistema irá gerar uma mensagem de voz: "*User number* **. *Registration is successful*". (Número de usuário **. Registro bem-sucedido) e pode-se seguir para o passo b; se o registro de impressão digital falhar, o sistema irá gerar uma mensagem de voz: "*Please press your finger again*". (Favor pressionar o dedo novamente) e retornará ao estado de registro, esperando a colocação do dedo ou a leitura do cartão.

b. Após gerar a seguinte mensagem de voz: "Registrer. Please press your finger or swipe your card" (Registrar. Favor colocar o dedo ou passar seu cartão), o sistema entra no estado de registro de informação de usuário especificado, esperando a nova leitura do cartão ID ou a colocação do dedo.

c. Se o registro do cartão ID for bem-sucedido, o sistema irá gerar uma solicitação de voz: "*Registration is successful. Please press your finger*" (Registro bem-sucedido. Favor pressionar dedo) e entra diretamente no estado de registro de impressão digital; se for colocado um dedo que não tenha sido registrado antes e for bem-sucedido no registro deste dedo, o sistema irá gerar uma solicitação de voz: "*Registration is successful. Please press your finger or swipe your card*" (Registro bem-sucedido. Favor colocar o dedo ou passar o seu cartão)" e pode-se continuar registrando novas impressões digitais e cartão. Após ter registrado 10 impressões digitais, o sistema irá gerar uma mensagem de voz: "Please swipe your card" (Favor passar seu cartão) para registrar seu cartão ID caso seu cartão ID não esteja registrado.

d. O sistema retorna automaticamente ao estado de verificação quando os 10 dedos e o cartão ID estiverem registrados, o cartão de gerenciamento for lido ou quando se atinge o tempo limite de operação.

3. Se já estiver registrado com um ID, então há duas formas para registrar suas impressões digitais ou cartão:

(1) Registrar impressões digitais quando já tiver registrado o cartão

a. Após fazer a leitura do cartão registrado, o sistema irá gerar uma mensagem de voz: "*User number* **. *Register. Please press your finger*" (Número de usuário **. Registrar. Favor pressionar seu dedo) (** Refere-se à ID designada a você; o mesmo abaixo) e entra no estado de registro de impressão digital. O registro de suas impressões digitais irá sobrescrever todas as impressões prévias.

b. Coloque o mesmo dedo sobre o sensor três vezes seguindo as solicitações de voz por adotar a colocação adequada do dedo. Se o registro de impressão digital for bem-sucedido, o sistema irá gerar a mensagem de voz: "*User number* **. *Registration is successful*". (Número de usuário **. Registro bem-sucedido) e fica pronto para o registro da próxima impressão digital.

c. O sistema retorna automaticamente ao estado de verificação quando os 10 dedos e o cartão ID são registrados, o cartão de gerenciamento é lido uma vez ou se atinge o tempo limite de operação.

Dicas:

1. As impressões digitais registradas neste passo irão sobrescrever todas as impressões digitais previamente registradas.

2. Neste modo, a impressão digital do usuário que possui o cartão de gerenciamento não pode ser registrada porque a leitura do cartão de gerenciamento retornará o sistema automaticamente para o estado de verificação.

(2) Registre o cartão e as impressões digitais quando já estiver registrado as impressões digitais.

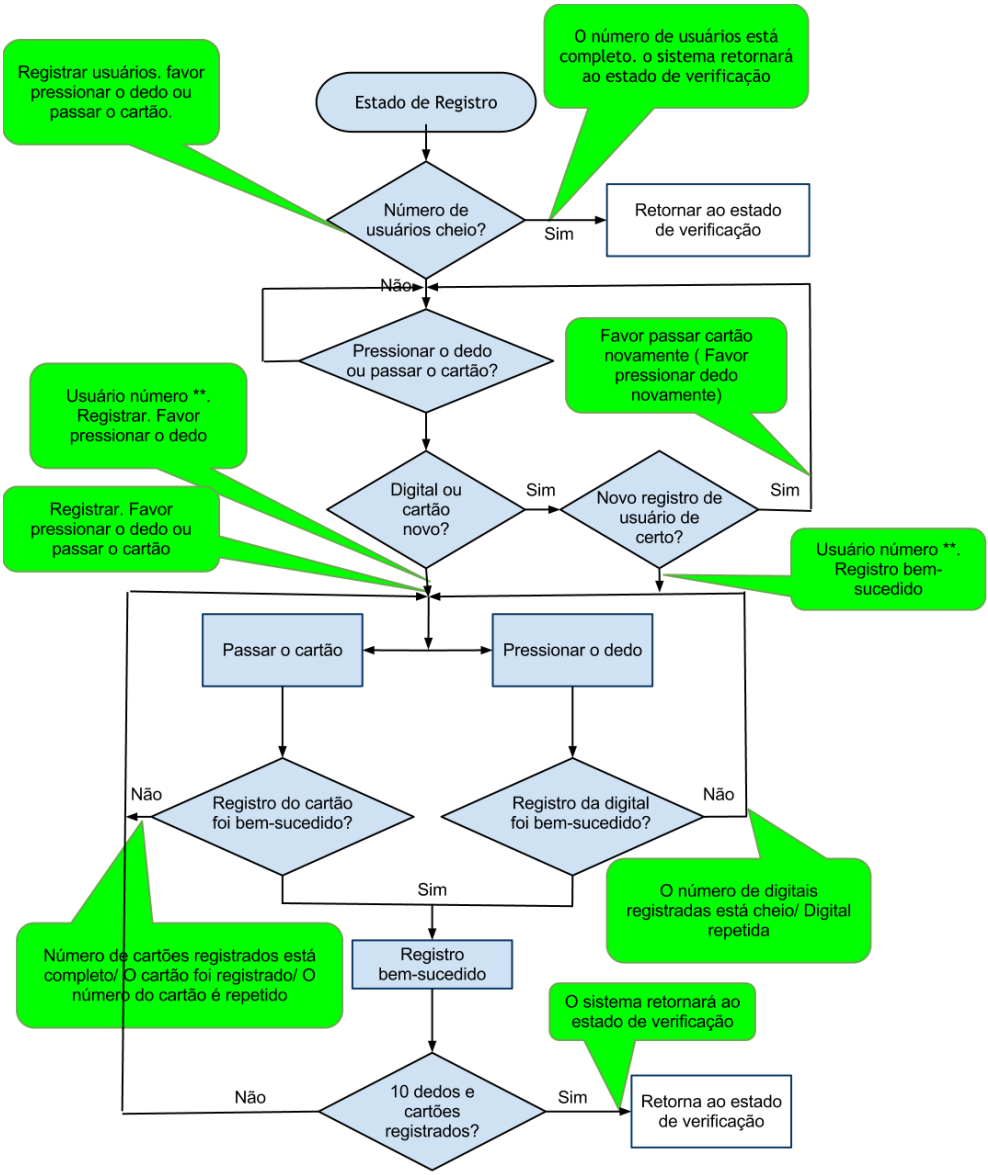
a. Coloque o dedo com a impressão digital já registrada três vezes seguindo as solicitações de voz. Se você for identificado como a mesma pessoa a cada tentativa de verificação, o sistema entra no estado de registro de impressão digital.

b. Após gerar a mensagem de voz ": *User number* **. *Register. Please press your finger or swipe your card*" (Número de usuário **. Registrar. Favor pressionar seu dedo ou passar o cartão)", o sistema começa a registrar sua impressão digital.
Sua impressão digital registrada neste passo irá sobrescrever todas as impressões digitais anteriores.

c. Se o registro de cartão ID for bem-sucedido, o sistema gera uma mensagem de voz: "*Registration is successful. Register. Please press your finger*"(Registro bem- sucedido. Registrar. Favor pressionar seu dedo) e entra diretamente no estado de registro de impressão digital; se você colocar um dedo que não esteja registrado anteriormente e for bem-sucedido no registro deste dedo, o sistema gera a seguinte mensagem de voz: "*Registration is successful. Please press your finger or swipe your card*" (Registro bem-sucedido. Favor passar seu dedo ou passar o cartão), e você pode continuar registrando novas impressões digitais e cartões. Após registrar 10 impressões digitais, o sistema irá gerar a seguinte mensagem de voz : "*Please swipe your card*" (Favor passar seu cartão) para registrar seu cartão ID se o mesmo não estiver registrado.

d. O sistema retorna automaticamente para o estado de verificação quando 10 dedos e os cartões ID são registrados, o cartão de gerenciamento é passado uma vez ou quando o tempo limite de operação é atingido.

O fluxograma é mostrado abaixo:

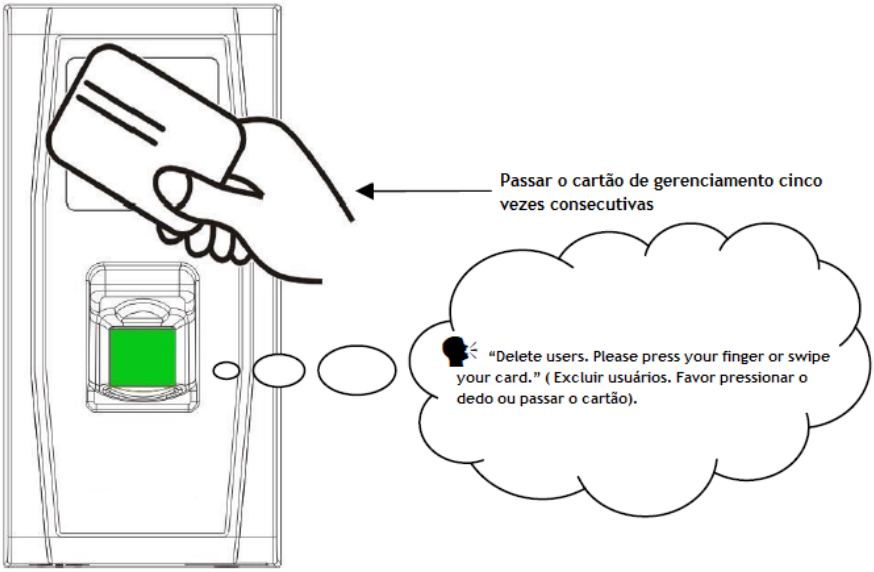


4.1.3 Excluir Usuário Simples

Excluir um usuário utilizando o cartão de gerenciamento é chamado de modo de exclusão de usuário simples. Excluir um usuário ao utilizar um teclado externo é chamado de modo de exclusão de usuário especificado.

Passos de operação para exclusão de usuário simples:

1. No estado de verificação, passe o cartão de gerenciamento cinco vezes consecutivas para entrar no estado de exclusão de usuário simples (passando o cartão mais uma vez retornará ao estado de verificação).



2. O sistema verifica se o usuário foi registrado. Se não, o sistema irá gerar a seguinte mensagem de voz: "*Unregistered user. The system returns to verification state*" (Usuário não registrado. O sistema retornará ao estado de verificação); caso contrário, o sistema irá gerar a seguinte mensagem de voz: "*Delete users. Please press your finge ror swipe your card*" (Excluir usuários. Favor pressionar seu dedo ou passar o cartão).
3. Coloque o dedo no sensor de impressão digital ou passe o cartão na leitora.

(1) Coloque o dedo no sensor para excluir um usuário.

Coloque um dos dedos registrados de modo adequado no sensor. Se a verificação der certo, o sistema irá gerar a mensagem de voz: "*User number **. Deletion is successful. Delete users. Please press your finger or swipe your card*" (Número de usuário **. Exclusão bem-sucedida. Excluindo usuários. Favor colocar o dedo ou passar o cartão) (** indica o número ID do usuário) e retorna automaticamente ao estado de exclusão.

Se a verificação falhar, o sistema irá gerar a seguinte mensagem de voz: "*Please press your finger again*" (Favor colocar o dedo novamente).

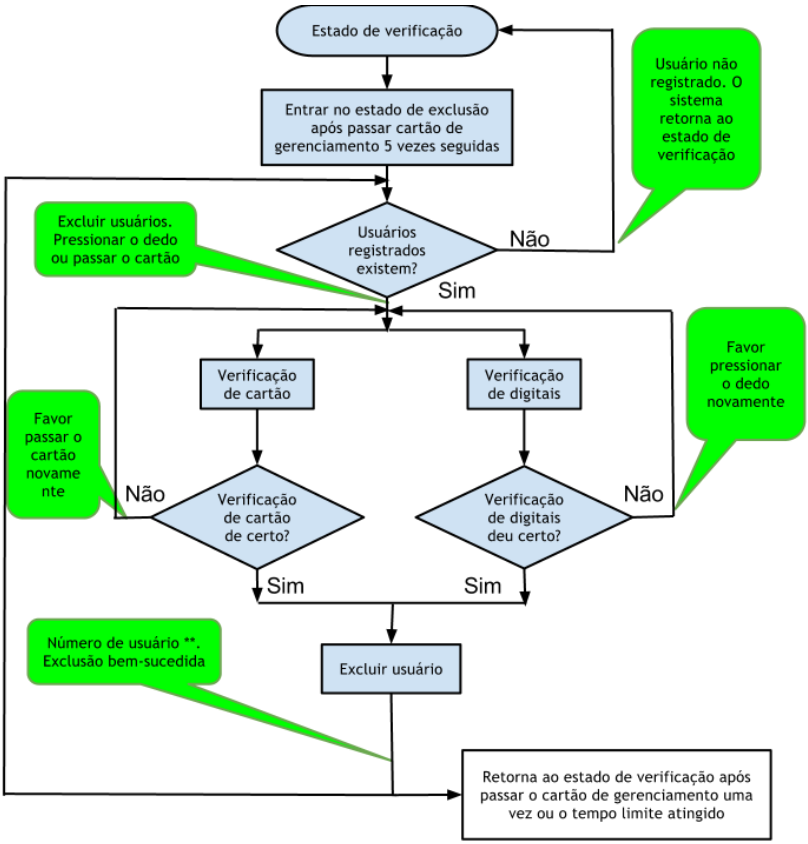
(2) Passar o cartão na leitora para excluir um usuário.

Passar um cartão registrado na leitora. Se a verificação der certo, o sistema irá gerar uma mensagem de voz: "*User number **. Deletion is successful. Delete users. Please press your finger or swipe your card*" (Número de usuário **. Exclusão bem-sucedida. Excluir usuários. Favor colocar o dedo ou passar o cartão). E retorna automaticamente ao estado de exclusão. Se a verificação falhar, o sistema irá gerar a seguinte mensagem de voz: " *Please swipe your card again*" (Favor passar o cartão novamente).

4. Se você passar o cartão de gerenciamento mais uma vez ou o tempo limite de operação for atingido, o sistema retornará ao estado de verificação.

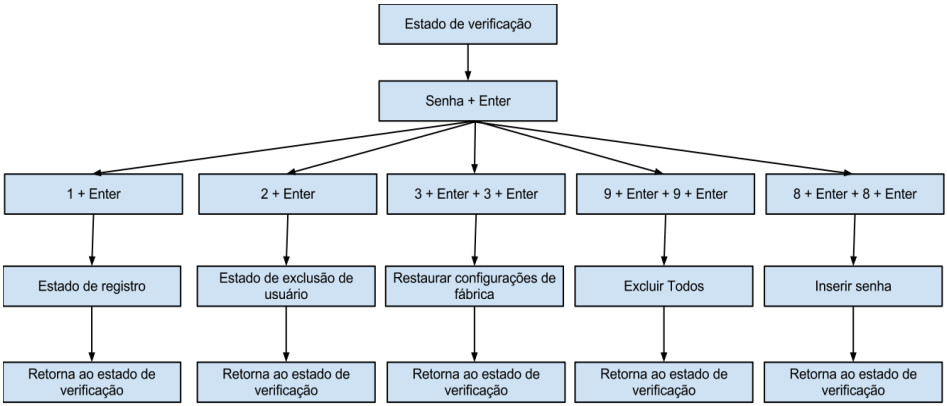
   - **Dica:** No modo de exclusão de usuário simples, usuários de cartão de gerenciamento não podem ser excluídos porque passar o cartão de gerenciamento fará o sistema retornar ao estado de verificação.

Procedimento de Exclusão de Usuário Simples:



4.1.4 Operações com Teclado USB

O fluxograma com as operações do teclado é mostrado abaixo:



4.1.5 Configurar Senha do Teclado

Se o usuário precisar de um teclado externo, basta ele conectar um teclado ao dispositivo e então passar o seu cartão de gerenciamento para ativar o teclado externo.

O sistema habilita o usuário para configurar uma senha dedicada para o teclado externo.

Passo de operação:

1. No estado de verificação, conectar um teclado externo ao dispositivo através da interface USB.

2. Passe seu cartão de gerenciamento uma vez para ativar o teclado. O sistema irá gerar uma mensagem de voz: "*Please press the keyboard*" *(*Favor pressionar o teclado*)*.

3. Digite "8" e pressione Enter. Depois digite "8" e pressione Enter novamente. O sistema irá gerar uma mensagem de voz: "*Please set password*" (Favor definir senha). Digite a senha desejada e pressione Enter. O sistema irá gerar a seguinte mensagem de voz: "*The operation is sucessful. The system retuns to verification state*" (Operação bem-sucedida. O sistema retorna ao estado de verificação). Se não houver eventos no teclado dentro de 30 segundos, o sistema irá gerar a mensagem de voz: "*Operation timeout. The system returns to verification state*" *(*Tempo limite de operação. O sistema retorna ao estado de verificação*)*. (A senha deve conter entre 4 e 6 dígitos).

O usuário pode digitar a senha para ativar as funções do teclado externo no próximo uso, ou passar o cartão de gerenciamento uma vez (que é obrigatório para o primeiro uso do teclado externo).

1. Se você entrar uma senha errada por seis vezes consecutivas, o teclado será bloqueado e o teclado terá de ser religado para seu desbloqueio.
2. Se não houver toques nas teclas dentro de 30 segundos após a ativação do teclado, as funções do teclado serão automaticamente desativadas e você deverá reativá-lo.
3. O teclado deve ser inserido ou removido em um intervalo de 15 segundos, caso contrário, o sistema não poderá identificar seu estado.

4.1.6 Registrar um Usuário Através do Teclado

Registrar um usuário usando o teclado USB chama-se modo de registro baseado no teclado. Neste modo, o usuário pode registrar um usuário com ID de usuário especificado.

Passos de Operação:

1. Conforme mostrado no fluxograma *3.2 USB Keyboard Operations*, digite "1" e pressione Enter para entrar no estado de registro.

2. Quando o sistema gerar a mensagem de voz: "*Register users. Please input the user number*" (Registrar usuários. Favor entrar com o número do usuário), entre com um ID de usuário.

3. O sistema gera a mensagem de voz: "*User number **. Register. Please press your finger or swipe your card*" (Número de usuário **. Registrar. Favor colocar o dedo ou passar o cartão). (** indica o número ID do usuário, mesmo abaixo). O sistema entra no estado de registro de ID especificado.

Dicas:

1. Se um usuário for registrado no sistema com cartão de gerenciamento, o sistema irá gerar a mensagem de voz: "*User number **. Please press your finger*" (Usuário número **. Favor colocar o dedo).

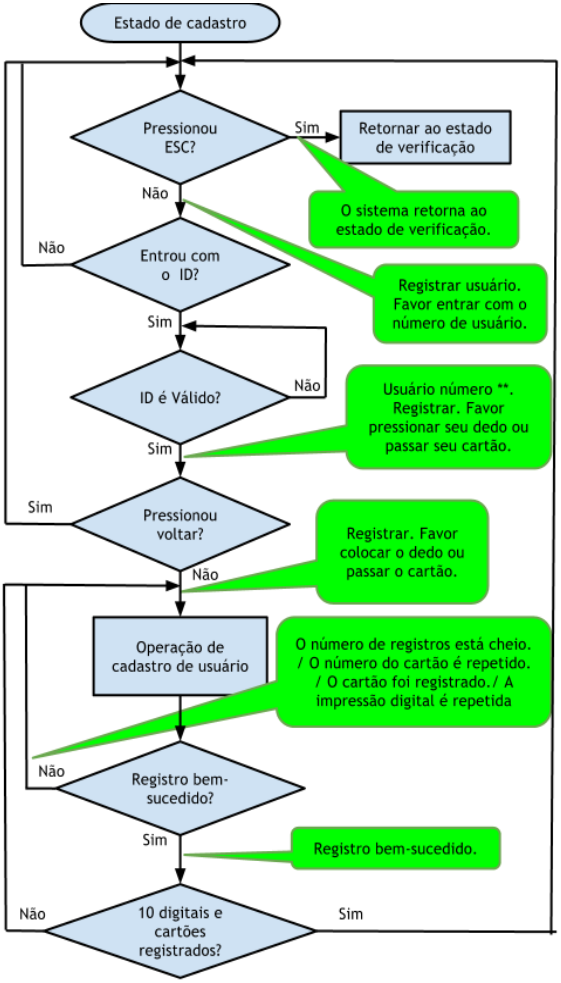
2. Se um usuário for registrado no sistema com um ID de usuário e 10 impressões digitais, o sistema irá gerar a mensagem de voz: "*User number **. Please swipe your card*" (Usuário número **. Favor passar o cartão).

4. A operação de registro de usuário no estado de registro de ID especificado é similar a operação de registro de ID especificado no modo de registro de cartão de gerenciamento. Para detalhes, ver 3.1.2 Registro de Usuário Simples.

5. No estado de espera de ID de usuário registrado, pressionar ESC para retornar ao estado de verificação. No estado de registro de ID de usuário especificado, pressione ESC duas vezes para retornar ao estado de verificação.

- **Dica:** No modo de registro baseado no teclado, podem-se registrar usuários consecutivamente. Quando o registro der certo, o sistema retorna automaticamente para o estado de registro.
-

O fluxograma de registro baseado no teclado é mostrado abaixo:



Informação Importante:

1. No modo de registro baseado em teclado, se qualquer operação chegar ao tempo limite, o sistema faz solicitação desta operação automaticamente uma vez a cada 10 segundos e retorna ao estado de verificação após fazer solicitação três vezes.

2. Impressões digitais recém-registradas irão sobrescrever todas as originais no modo de registro baseado no cartão de gerenciamento, bem como no modo de registro baseado no teclado.

3. Um usuário só pode registrar um cartão. Quando o usuário com um cartão registrado se registra no sistema, o sistema gera a mensagem de voz: "*Register. Please press your finger*" (Registrar. Favor colocar o dedo). Quando o usuário passa o cartão, o sistema gera a solicitação de voz: "*The card has been registered*" (O cartão foi registrado).

4. Um cartão não pode ser registrado repetidamente, caso contrário, o sistema irá gerar a mensagem de voz: "*The card number is repeated*" (O número do cartão é repetido). Durante a passagem do cartão. Usuários diferentes não podem registrar a mesma impressão digital, caso contrário, o sistema irá gerar a mensagem de voz: "*The fingerprint is repeated*" (A impressão digital é repetida). Durante o registro da impressão digital. As novas impressões digitais do usuário irão sobrescrever as existentes.

4.1.7 Excluir um Usuário Especificado

Excluir um usuário ao usar um teclado externo chama-se modo de exclusão de usuário especificado.

Passos de Operação:

1. Conecte um teclado USB ao dispositivo e passe seu cartão de gerenciamento uma vez ou insira sua senha para ativar o teclado.

2. Digite "2" e pressione Enter para entrar no modo de exclusão de usuário especificado. O sistema verifica se existem quaisquer usuários registrados.

3. Se houver quaisquer usuários registrados, o sistema irá gerar a mensagem de voz: "*Delete users. Please input the user number*"(Excluir usuários. Favor inserir número de usuário). E pode-se dar sequência ao próximo passo, caso contrário, o sistema irá gerar a seguinte mensagem de voz: "*Unregistered user. The system returns to verification state*" (Usuário não registrado. O sistema retornará ao estado de verificação).

4. Insira um ID de usuário e o sistema verifica se o ID de usuário é válido.

5. Se o ID de usuário for válido, o sistema irá gerar a solicitação de voz: "*User number **. Deletion is successful. Delete users. Please input the user number*" (Usuário número **. Exclusão bem-sucedida. Excluir usuários. Favor inserir o número de usuário). E retorna automaticamente ao estado de exclusão. Se o ID de usuário for inválido, o sistema irá gerar a solicitação de voz: "*Wrong user ID*" (ID de usuário errado).

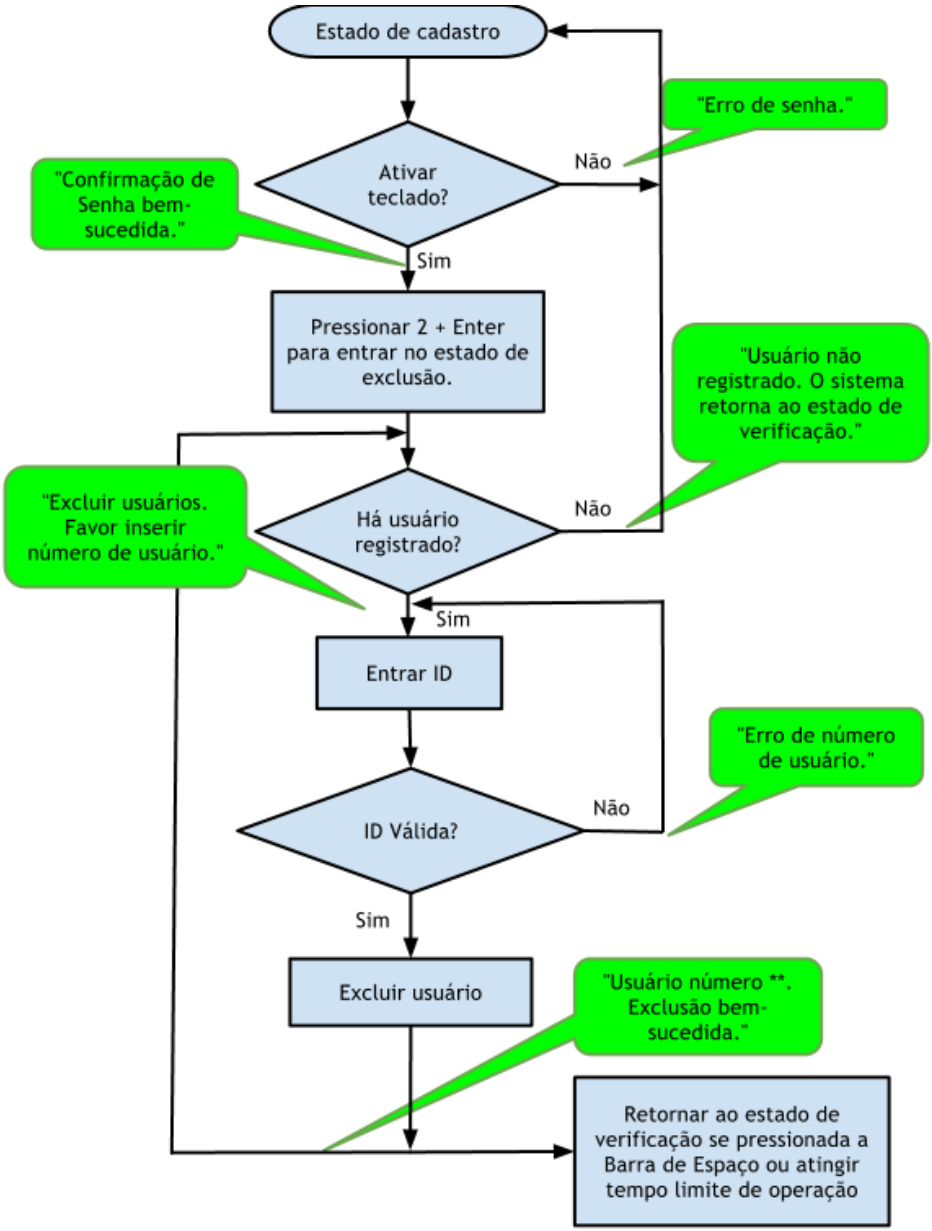
6. Se você pressionar ESC ou se o tempo limite de operação for atingido, o sistema retornará ao estado de verificação.

Dicas:

1. No modo de exclusão de usuário especificado, IDs de usuário e IDs de usuários de cartões de gerenciamento que estiverem registrados no sistema são todos considerados inválidos.

2. No modo de exclusão baseado no teclado, o sistema bloqueia o sensor de impressão digital e a leitora do cartão e, portanto, qualquer operação neles é inválida.

O fluxograma de exclusão de usuário especifica é mostrado abaixo:



4.1.8 Excluir Todos os Usuários

Passos de Operação:

1. Conecte o teclado USB ao dispositivo e passe o cartão de gerenciamento na leitora uma vez ou insira sua senha para ativar o teclado.

2. Digite "9" e pressione Enter. Então, digite "9" e pressione Enter novamente. O sistema exclui todos os usuários.

3. Se a operação der certo, o sistema irá gerar a solicitação de voz: "*Delete all users. The operation is successful. The system returns to verification state. Please register the management card*" (Excluir todos os usuários. A operação foi bem-sucedida. O sistema retornará ao estado de verificação. Favor registrar o cartão de gerenciamento)".

Dicas:

1. Você pode excluir um cartão de gerenciamento usando a função Excluir Todos.

2. Você pode usar a função Excluir Todos para excluir todos os usuários registrados, impressões digitais e registros.

3. Muita atenção nesse procedimento, pois, uma vez excluídos, os dados não podem ser mais recuperados.

4.1.9 Restaurar Configurações de Fábrica

Passos de Operação:

1. Conecte um teclado USB ao dispositivo e passe o cartão de gerenciamento uma vez ou insira sua senha para ativar o teclado.

2. Digite "3" e pressione Enter. Então digite "3" e pressione Enter novamente. O sistema restaura as configurações de fábrica.

3. Após o êxito da operação, o sistema gera o aviso de voz: "*Restore to default settings. The operation is successful. The system returns to verification state*" (Restaurar configurações de fábrica. A operação foi bem-sucedida. O sistema retornará ao estado de verificação).

Pode-se também restaurar as configurações de fábrica ao reiniciar a chave tamper. Ver 3.5 Chave Tamper.

Após o dispositivo ser restaurado às configurações de fábrica, as informações do dispositivo são restauradas por àquelas que vêm de fábrica, incluíndo o número do dispositivo, senha do sistema, endereço de IP, endereço 485 e senha de teclado.

- **Aviso:** A informação de usuário armazenada no dispositivo não será apagada após o dispositivo ter sido restaurado às configurações de fábrica.

4.2 Verificação de Usuário

Passos de Operação:

1. Quando o dispositivo estiver no estado de verificação, o sistema gera o aviso de voz: "*Verify users. Please press your finger or swipe your card*" (Verificar usuários. Favor pressionar seu dedo ou passar o cartão).

2. Iniciar verificação de usuário. O dispositivo suporta dois modos de verificação: Verificação de impressão digital e Verificação de cartão.

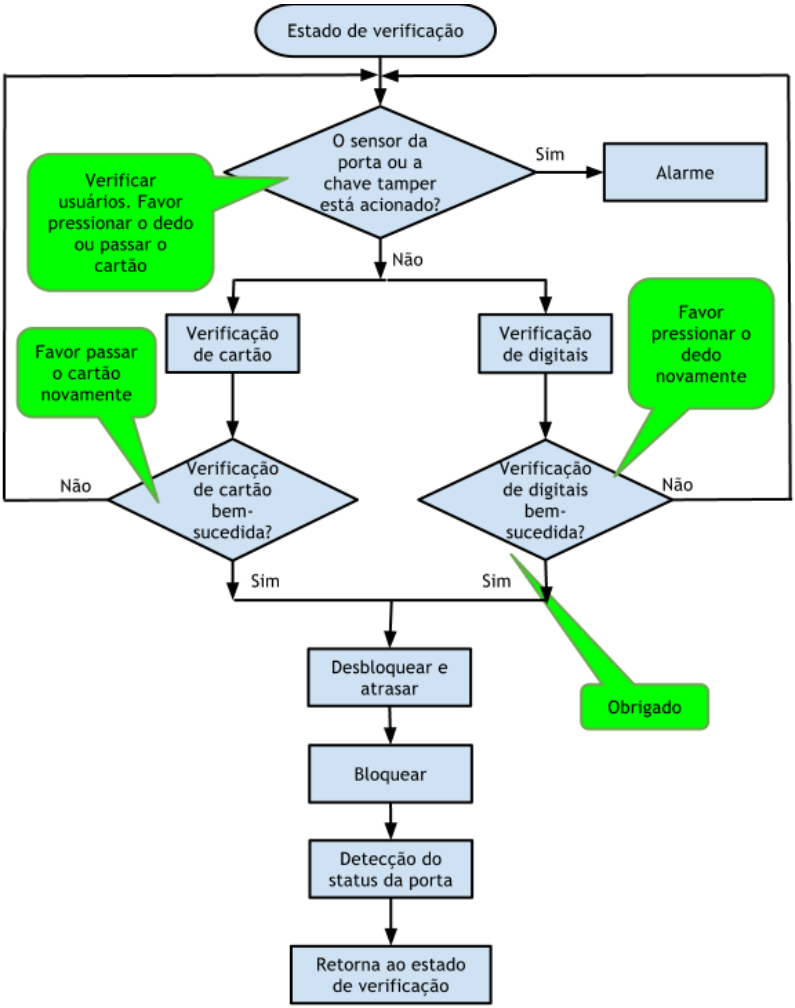
(1) Verificação de impressão digital

Coloque seu dedo adequadamente no sensor de impressão digital. Se a verificação der certo, o sistema gera o aviso de voz: "*Thank you*" (Obrigado). E simultaneamente aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gera o aviso de voz: "*Please press your finger again*" (Favor colocar o dedo novamente).

(2) Verificação de cartão

Passe seu cartão na leitora de cartão. Se a verificação der certo, o sistema gera o aviso de voz: "*Thank you*" (Obrigado). E simultaneamente aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gera o aviso de voz: "*Please swipe your card again*" (Favor passar o cartão novamente).

O fluxograma da verificação de usuário é mostrado abaixo:



- **Dica:** O usuário pode desbloquear por usar suas impressões digitais registradas em vez de o cartão de gerenciamento.

4.3 Entrada USB

O usuário pode realizar download de registro, download de usuário, upload de usuário e atualização do firmware através de uma entrada USB.

a. Download de registro (Download Records): Download dos registros de assistência de todos os usuários a partir do dispositivo para um entrada USB.

b. Download de usuário (Download Users): Download de todas as informações do usuário, tais como; impressões digitais e números de cartões do dispositivo para um entrada USB.

c. Upload de usuário (Upload Users): Upload da informação de usuário de um entrada USB para o dispositivo.

d. Atualização de Firmware (Upload Firmware): Atualização do firmware do dispositivo através de um entrada USB.

Os arquivos de configuração na entrada USB podem ser criados e modificados usando o software de gerenciamento de controle de acesso. Execute o software de gerenciamento de controle de acesso e proceda da seguinte forma:

1. Escolher Gerenciamento de Dispositivo > Configuração de entrada USB para acessar a interface de operação.

2. Selecionar entrada USB no menu suspenso para mostrar quatro itens: Download de registros, Download de usuários, Upload de usuários e Atualização de firmware.

3. Selecione a opção desejada e clique em Aplicar. Quando o sistema mostrar a mensagem "Operação completada", o arquivo de configuração operatemode.cfg está criado na entrada USB.

As operações com entrada USB incluem os dois casos seguintes:

1. Se você conectar uma entrada USB sem arquivo de configuração ao dispositivo, o system automaticamente apresentará mensagens de sequência de operação.

(1) Após conectar a entrada USB ao dispositivo, pode-se passar o cartão uma vez para entrar no estado de gerenciamento da entrada USB.

(2) O sistema gera a mensagem de voz: "****. *Please swipe your management card for confirmation*" (****. Favor passar seu cartão de gerenciamento para confirmação). (**** indica os quatro itens de operação de **a** até **d** em sequência, conforme ordem acima).

(3) Se quiser realizar o gerenciamento da entrada USB, passe o cartão para confirmação. Se a operação der certo, o sistema gera a mensagem de voz: "*The operation successful*" (A operação foi bem-sucedida). E o levará a seguir para o próximo passo. Após terminar os quarto itens, o sistema gera a mensagem de voz: "The system returns to verification state" (O sistema retorna ao estado de verificação). Se a operação falhar, o sistema gera a mensagem de voz: "The operation fails. The system returns to verification state" (A operação falhou. O sistema retornará ao estado de verificação).

(4) Se você não passar o cartão de gerenciamento, o sistema automaticamente pulará este passo em 5 segundos e o conduzirá ao próximo passo. Após o término dos quatro itens, o sistema retorna ao estado de verificação automaticamente.

2. Se conectar uma entrada USB com arquivo de configuração ao dispositivo, o sistema executará operações com base nas configurações do arquivo de configuração.

(1) Após conectar a entrada USB ao dispositivo, pode-se passar o cartão uma vez para entrar no estado de gerenciamento da entrada USB.

(2) O sistema obtém comandos de operação por ler o arquivo de configuração na entrada USB e gera a mensagem de voz: "Run configuration files in the U-disk. Please swipe your management card for confirmation" (Executar arquivos de configuração na entrada USB. Favor passar o cartão de gerenciamento para confirmação).

(3) Após passar o cartão e realizar todas as operações com sucesso, o sistema gera a mensagem de voz: "****. The operation is successful." (****. A operação foi bem-sucedida). Na sequência de cada passo da operação. Se

quaisquer das operações falharem, o sistema gera a mensagem de voz: "***. The operation fails. (****. Falha na operação).

(4) Após o término de todas as operações, o sistema gera a mensagem de voz: "The system returns to verification state" (O sistema retornará ao estado de verificação).

4.4 Chave Tamper

A chave tamper é pressionada e mantida assim com uma cobertura traseira neste estado por meio da cobertura traseira. Quando o dispositivo é desmontado, a chave tamper será acionada e enviará um sinal de alarme para desencadear um alarme.

Limpar alarme: O usuário pode limpar o alarme por desbloquear a porta com a combinação certa.

Especificações		
Capacidade de armazenamento de digitais		1.500
Capacidade de armazenamento de cartões		10.000
Armazenamento de logs		100.000
Comunicação		TCP/IP e RS485
Tensão de Alimentação		12VCC
Corrente de Consumo (mA)	Estado normal	328
	Alternando os Menus	341
	Verificando imp. Digital/cartão	345
	Relé atuando	352
	Modo stand by	235
	Inicializando	400
Temperatura de operação		0° ~ +45°
Umidade relativa		10% ~ 90%
Dimensões (LxAxP)		73x148x34,5mm
Peso aproximado		1,15kg
Campainha		Contato seco
Botão de Saída		NA
Alarme		Contato seco
Tamper		Sim
Sensor de porta aberta		NA/NF
Saída para fechadura		NA/C/NF
Grau de proteção		IP65
Entrada USB		Download / Upload / Teclado Externo

Certificado de Garantia

1- Todas as partes, peças e componentes, são garantidos contra eventuais DEFEITOS DE FABRICAÇÃO que porventura venham a apresentar, pelo prazo de 1 (um) ano, contado a partir da data de emissão da nota fiscal do produto.

2- Constatado o defeito, deve-se imediatamente comunicar à empresa que efetuou a instalação ou serviço autorizado mais próximo. Somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia. Caso contrário esta garantia perde o efeito, pois o produto terá sido violado.

3- Em caso de atendimento domiciliar e/ou necessidade de retirada do produto, as despesas decorrentes de serviços, transporte, segurança de ida e volta do produto, ficam por conta e risco do consumidor.

4- A garantia ficará automaticamente cancelada se o produto for violado, receber maus tratos ou sofrer danos decorrentes de acidentes, quedas, agentes da natureza (raios, inundações), variações de tensão elétrica, sobrecarga acima do especificado e instalação em desacordo com o manual.

LOCAL: _____

REVENDA: _____

DATA: _____

Importado por: Khronos Indústria, Comércio e Serviço em Eletrônica LTDA. CNPJ 78.323.094/0004-70.

Fabricante:
DONGGUAN ZKTECO ELECTRONIC TECHNOLOGY CO., LTD.
PINGSHAN 188 INDUSTRY ZONE 26 TANGXIA TOWN DONGGUAN - CHINA

ANATEL
Agência Nacional de Telecomunicações
4688-15-7632
MODELO: A08

"Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo e não pode causar interferência a sistemas operando em caráter primário."

Informações e suporte técnico do produto:
www.cs.ind.br suporte@cs.ind.br

CS COMUNICAÇÃO E SEGURANÇA
Fone: +55 (48) 3246-8563

CS
COMUNICAÇÃO E SEGURANÇA

02.009.032.004.01

A CS Comunicação e Segurança fornece este documento no estado em que se encontra, não oferecendo nenhuma garantia quanto à precisão das informações fornecidas e se exime de qualquer responsabilidade por danos e prejuízos resultantes do seu uso.