

NOTA DE APLICAÇÃO

Leituras e gravações criptografadas

Atmel CryptoAuthentication

Introdução

A linha de produtos Atmel® CryptoAuthentication™ oferece uma maneira excepcionalmente limpa de manter o tráfego entre o dispositivo CryptoAuthentication e o microcontrolador criptografado para evitar espionagem no barramento durante a personalização ou operação do sistema. A leitura criptografada e a gravação criptografada são configurações dos comandos Read e Write e fornecem um mecanismo para limitar o acesso, habilitar recursos ou atualizar um valor de chave.

Características

• Armazene senhas ou chaves com segurança sem transferir os valores em claro • Verifique a senha ou chaves sem revelar o valor esperado

1 Visão geral

Dispositivos de hardware seguros podem fornecer mecanismos para ocultar o valor claro da senha, evitar ataques exaustivos off-line e aumentar consideravelmente a dificuldade de ataques físicos locais. O Atmel®

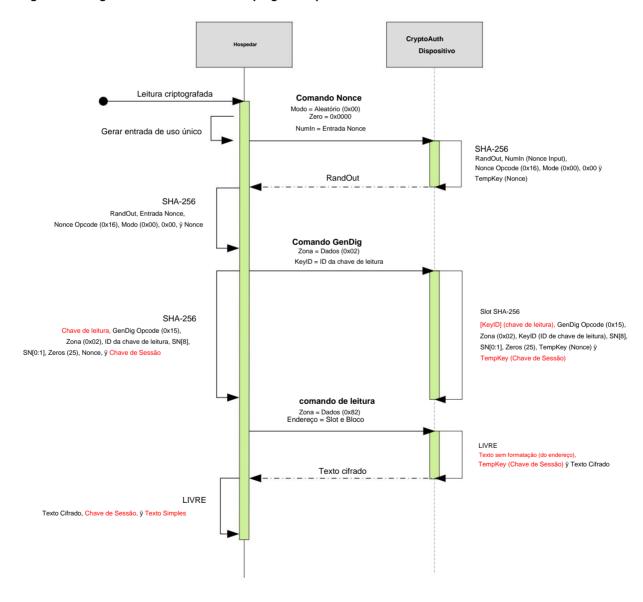
Os dispositivos CryptoAuthentication™ (dispositivos criptográficos) fornecem essa capacidade em um pacote muito pequeno e a um custo baixo, fácil de integrar em qualquer sistema digital.

Existem algumas maneiras de implementar os comandos de leitura criptografada ou gravação criptografada.

2 Leitura criptografada

2.1 Leitura criptografada padrão

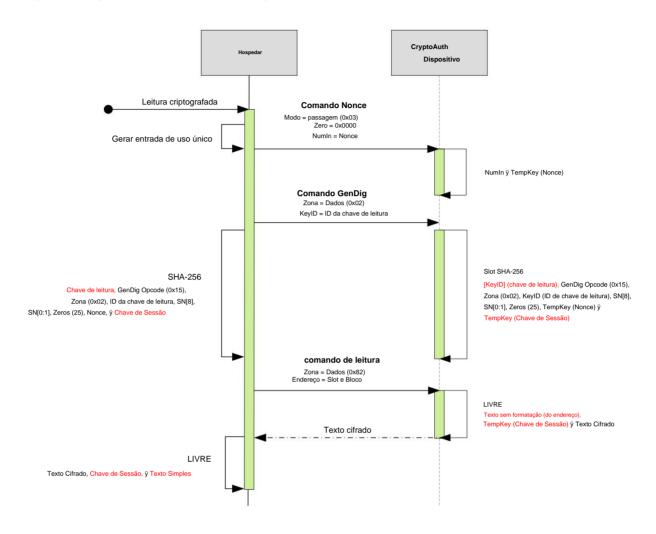
Figura 2-1. Diagrama de fluxo de leitura criptografada padrão





2.2 Leitura criptografada simples

Figura 2-2. Diagrama de Fluxo de Leitura Criptografada Simples

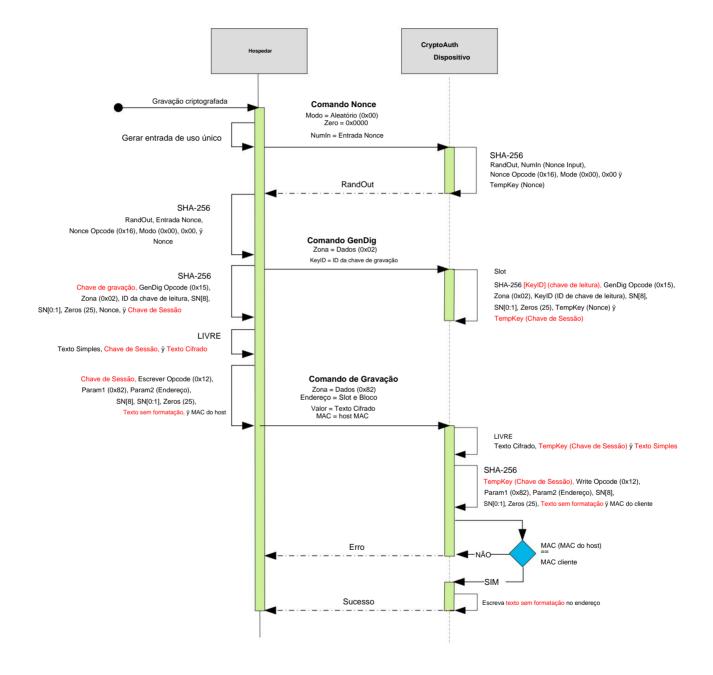




3 Gravação Criptografada

3.1 Gravação criptografada padrão

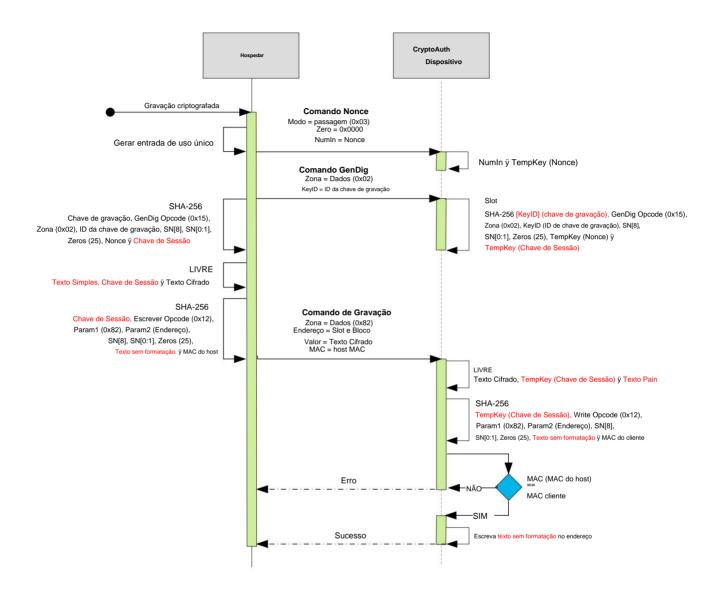
Figura 3-1. Diagrama de Fluxo de Gravação Criptografado Padrão





3.2 Gravações criptografadas simples

Figura 3-2. Diagrama de Fluxo de Gravações Criptografadas Simples





4 Configuração Antes

de usar o dispositivo Atmel ATSHA204A para criptografia, há processos de inicialização que devem ser executados. Os processos de inicialização consistem em personalizar e depois bloquear o dispositivo. Na etapa de personalização, o comportamento do dispositivo, o comportamento do slot de dados e os próprios dados são configurados conforme desejado.

Após a realização do processo de personalização, o dispositivo é bloqueado para que a configuração entre em vigor e para evitar qualquer alteração posterior nos dados. Esta seção descreve maneiras de configurar o dispositivo para cada esquema de criptografia específico.

4.1 Leitura criptografada padrão e leitura criptografada simples

Tabela 4-1. Leitura criptografada padrão e leitura criptografada simples

Hospedar	NOVO 204A
Gerar entrada Nonce (Numln).	1. Defina:
2. Salve ReadKeyID e ReadKey.	 SlotConfig.ReadKey (ReadKeyID)
	SlotConfig.EncryptRead •
	SlotConfig.IsSecret 2. Lock
	Config Zone 3. Carregar
	ReadKey no Slot[ReadKeyID]
	4. Bloquear zona de dados

Notas: 1. A leitura criptografada aplica-se apenas à leitura de 32 bytes.

- 2. Para leitura criptografada padrão, ReadKeyID pode ser par ou ímpar. Se ReadKeyID for ímpar, o bit CheckMacConfig correspondente ao Slot a ler deve ser zero
- 3. Para leitura criptografada simples, ReadKeyID deve ser ímpar e o bit CheckMacConfig correspondente ao Slot a ler não deve ser zero.

4.2 Gravação Criptografada Padrão e Gravação Criptografada Simples

Tabela 4-2. Gravação criptografada padrão e gravação criptografada simples

Hospedar	NOVO 204A
Gerar entrada Nonce (Numln).	1. Defina:
Salve WriteKeyID e WriteKey.	 SlotConfig.WriteKey (WriteKeyID)
	SlotConfig.IsSecret • Bit 14
	de SlotConfig
	2. Zona de configuração de bloqueio
	3. Carregar WriteKey no slot [WriteKeyID]
	4. Bloquear zona de dados

Notas: 1. Gravação criptografada aplica-se apenas à gravação de 32 bytes.

- 2. Se a zona de dados estiver desbloqueada, o parâmetro 1 do comando de gravação é usado para indicar se os dados de entrada são ou não criptografado.
- 3. Para gravação criptografada padrão, WriteKeyID pode ser ímpar ou par. Se WriteKeyID for ímpar, o bit CheckMacConfig correspondente ao Slot a Gravar deve ser zero.
- 4. Para Gravação Criptografada Simples, WriteKeyID deve ser ímpar e o bit CheckMacConfig correspondente ao Slot a Gravar não deve ser zero.



5 Histórico de Revisão

Doutor Rev.	Data	Comentários
8981B	10/2015	Corrigido o diagrama de fluxo de gravação criptografado padrão.
8981A	09/2015	Liberação inicial do documento.















Atmel Corporation

1600 Technology Drive, San Jose, CA 95110 USA T: (+1)(408) 441.0311

F: (+1)(408) 436.4200

www.atmel.com

© 2015 Atmel Corporation. / Rev.:Atmel-8981B-CryptoAuth-Encrypted-Reads-Writes-ApplicationNote_102015.

Atmel® , Logotipo da Atmel e suas combinações, Enabling Unlimited Possibilities® , CryptoAuthentication™ e outras são marcas registradas ou marcas comerciais da Atmel Corporation nos EUA e em outros países. Outros termos e nomes de produtos podem ser marcas comerciais de terceiros.

ISENÇÃO DE RESPONSABILIDADE: As informações neste documento são fornecidas em relação aos produtos Atmel. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, para qualquer direito de propriedade intellectual é concedida por este documento ou em conexão com a venda de produtos Atmel. EXCETO CONFORME ESTABELECIDO NOS TERMOS E CONDIÇÕES DE VENDAS DA ATMEL LOCALIZADOS NO SITE DA ATMEL. A ATMEL NÃO ASSUME NENHUMA RESPONSABILIDADE E RENUNCIA A QUALQUER GARANTIA EXPRESSA, IMPLÍCITA OU LEGAL RELACIONADA A SEÚS PRODUTOS, INCLUINDO, SEM LIMITAÇÃO, A GARANTIA IMPLÍCITA DE COMERCIABILIDADE, ADEQUAÇÃO PARA UMA FINALIDADE ESPECÍFICA OU NÃO VIOLAÇÃO. EM NENHUM CASO A ATMEL SERÁ RESPONSÁVEL POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENTES, PUNITIVOS. ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDAS E LUCROS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) DECORRENTES DO USO OU INCAPACIDADE DE USE ESTE DOCUMENTO, MESMO SE A ATMEL TIVER SIDO AVISADA DA POSSIBILIDADE DE TAIS DANOS. A Atmel não faz representações ou garantias com relação à precisão ou integridade do conteúdo deste documento e reserva-se o direito de fazer alterações nas específicações e descrições de produtos a qualquer momento sem aviso prévio. A Atmel não se compromete a atualizar as informações aqui contidas. Salvo disposição em contrário, os produtos Atmel não são adequados e não devem ser usados em aplicações automotivas. Os produtos Atmel não são destinados, autorizados ou garantidos para uso como componentes em aplicações destinadas a dar suporte ou

ISENÇÃO DE RESPONSABILIDADE PARA APLICAÇÕES DE SEGURANÇA CRÍTICA, MILITAR E AUTOMOTIVA: Os produtos da Atmel não são projetados e não serão usados em conexão com quaisquer aplicações em que se espera que a falha de tais produtos resulte em ferimentos pessoais significativos ou morte ("Segurança - Critical Applications") sem o consentimento específico por escrito de um funcionário da Atmel. Aplicações críticas de segurança incluem, sem limitação, dispositivos e sistemas de suporte à vida, equipamentos ou sistemas para a operação de instalações nucleares e sistemas de armas. Os projectadus:invepsioutputiojsstultuleksnoetscelessisspeliogspäine