



Migrando AT88SA102S para ATSHA204

Características

- Configuração do Atmel® ATSHA204 para compatibilidade de hardware com o Atmel AT88SA102S

- A compatibilidade de autenticação ATSHA204 com o AT88SA102S •

A compatibilidade de leitura ATSHA204 com o AT88SA102S Fuse Read

Descrição

Esta nota de aplicação descreve como configurar o ATSHA204 para que o dispositivo possa atuar como uma substituição AT88SA102S.

Como membros da família Atmel CryptoAuthentication™, o AT88SA102S e o

Os dispositivos ATSHA204 usam o algoritmo SHA-256 para autenticação do sistema, chave armazenamento/troca e outros usos relacionados. Enquanto o ATSHA204 oferece uma ampla gama de recursos e armazenamento EEPROM, foi projetado para ser compatível com versões anteriores do AT88SA102S. A maioria dos sistemas aplicativos projetados para usar o AT88SA102S pode ser facilmente atualizado para usar o ATSHA204 sem exigir nenhuma alteração de hardware ou software em o Host ou Cliente.

O pacote é idêntico para todos os dispositivos assim como o protocolo I/O; então nenhuma mudança de placa é necessário nem nenhuma alteração necessária para os drivers de E/S de baixo nível.

1. Compatibilidade de autenticação ATSHA204

O ATSHA204 foi projetado para ser compatível com o AT88SA102S para operação em campo. A maioria dos sistemas projetados para usar o AT88SA102S em dispositivos Cliente funcionará perfeitamente com o ATSHA204 nos dispositivos Cliente sem nenhuma modificação no software ou hardware do sistema Host.

Ao usar o AT88SA102S para autenticação, um comando MAC é executado e a resposta é comparada a um cálculo idêntico no Host. O dispositivo ATSHA204 pode ser configurado de modo que seu comando MAC corresponda à resposta MAC AT88SA102S para todos os modos.

1.1 Configuração ATSHA204

Para compatibilidade com o AT88SA102S, os seguintes valores devem ser gravados na memória do ATSHA204:

1. Durante a configuração, OTPmode deve ser definido como Legacy para ocultar os valores dos primeiros 64 bits do OTP seção, que contém um segredo no AT88SA102S.
2. As mesmas informações secretas e de status que seriam gravadas nos primeiros 88 bits de fusível do AT88SA102S devem ser gravadas nos primeiros 88 bits da seção OTP no ATSHA204.
3. Os bits OTP 88 a 95 devem ser escritos com o valor armazenado em SN[8] dentro da zona de configuração do dispositivo ATSHA204. O comando Read em sistemas legados sempre usará os valores na zona OTP, enquanto o ATSHA204 sempre usará os valores na zona Configuration durante a computação dos resultados criptográficos.
4. Os bits OTP 96 a 127 devem ser escritos com cópias dos valores armazenados em SN[4:7] dentro da zona de configuração do dispositivo ATSHA204.
5. O slot de chave identificado pelos quatro bits menos significativos do AT88SA102S SlotID atribuído a um determinado customer deve ser carregado com o valor fornecido pela Atmel para essa chave.
6. Os bits SlotConfig para o slot de chave identificado na Etapa 5 devem ser definidos como: CheckOnly=0, SingleUse=0, EncryptRead=0, IsSecret=1, WriteConfig=1000.

1.1.2 Modo OTP definido como *legado*

A configuração do modo OTP na zona de configuração deve ser definida como modo legado (0x00).

0x00 (modo legado) = quando a zona OTP está bloqueada, as gravações são desativadas, as leituras para a palavra 0 e a palavra 1 e as leituras de 32 bytes estão desativados.

1.1.3 Mapa de bytes da zona OTP

As questões a considerar ao configurar a zona OTP no ATSHA204 são para duplicar o MAC existente e os comandos Fuse Read para o AT88SA102S. O comando Fuse Read para o AT88SA102S usa o modo = 01.

corresponde a uma Zona OTP lida no ATSHA204.

A zona OTP do ATSHA204 deve ser configurada da seguinte forma:

Figura 1-1. Configuração de Zona ATSHA204 OTP

| Byte | Contagem de bytes OTP | fusíveis (bits) | Descrição |
|------|-----------------------|--|--|
| 8 | 0x00 – 0x07 | 0 – 63 AT88SA102S Fusíveis Secretos + Bit de Habilitação de BurnFuse | |
| 3 | 0x08 – 0x0A | 64 – 83 23 Status Fusíveis + Bit de Desativação de Fusível. | |
| 1 | 0x0B | 88 – 95 | AT88SA102S: Fusível MfrID (8 bits). (1) ATSHA204: SN[8]. Copiado da zona de configuração. |
| 4 | 0x0C-0x0F | 96 – 127 | AT88SA102S: Fusível SN (32 bits) ATSHA204: SN[4:7]. Copiado da zona de configuração. (1) |

Observação: 1. Os bytes SN de cada dispositivo precisam ser copiados da zona de configuração para o local designado na zona OTP. Isso garante que os comandos de leitura do AT88SA102S se comportem de forma idêntica.

1.1.4 Configuração de chave-valor

Os valores armazenados na matriz de chaves interna do AT88SA102S são conectados às camadas de máscara do dispositivo durante a fabricação do wafer. O ID de chave individual e os valores de chave correspondentes são disponibilizados para clientes qualificados mediante solicitação à Atmel.

O ATSHA204 *não* possui valores de chave interna; portanto, o valor da chave interna do AT88SA102S deve ser explicitamente programado em um slot específico de chave no ATSHA204.

Siga estas etapas para configurar as chaves internas AT88SA102S para ATSHA204:

1. Mascare o ID da chave AT88SA102S para determinar o slot. (Veja exemplos abaixo)
2. Escreva o valor da chave obtido da Atmel no slot indicado na Etapa 1.

O comando MAC do ATSHA204 irá mascarar todos menos os quatro bits menos significativos do KeyID (Param2). Param2 aparecerá primeiro no byte menos significativo do barramento. Abaixo estão alguns exemplos.

Figura 1-2. Exemplos

| AT88SA102S ID da chave | Parâmetro 2 (No ônibus) | ATSHA204 slot |
|---------------------------|----------------------------|------------------|
| 5492 | 9254 | 2 |
| 7D8E | 8E7D | E |

1.2 Cálculo de Autenticação ATSHA204

Depois que o ATSHA204 estiver configurado corretamente, o resultado de seu comando MAC corresponderá ao comando MAC AT88SA102S para todos os modos. A mensagem enviada para o cálculo do SHA-256 é ilustrada na tabela a seguir.

Tabela 1-1. Bytes de mensagem para cálculo de SHA-256

| Byte Contagem | AT88SA102S | ATSHA204 | Exemplo bytes | Notas |
|---------------|--------------------|--------------------|---------------|---|
| 32 (256 bits) | chave[KeyID] | key[KeyID] | 00 01...1E 1F | AT88SA102S: Chave interna da Atmel. ATSHA204: Slot tem o mesmo valor da chave interna AT88SA102S. |
| 32 (256 bits) | Desafio | Desafio | 10 11...2E 2F | O sistema pode enviar qualquer byte para desafio. |
| 1 (8 bits) | Código de operação | Código de operação | 08 | O opcode MAC é o mesmo para ambos os dispositivos. |
| 1 (8 bits) | Modo | Modo | 50 | Bit 4: Inclui 88 bits OTP (OTP[0:10]) na mensagem. Bit 6: Inclui 48 bits SN (SN[2:3] & SN[4:7]) na mensagem. |
| 2 (16 bits) | KeyID | Parâmetro 2 | 92 E3 | Byte menos significativo primeiro no barramento. Nota: O KeyID completo deve ser enviado para o ATSHA204. |
| 8 (64 bits) | fusíveis secretos | OTP[0:7] | 20 21...26 27 | Segredo programável |
| 3 (24 bits) | Fusíveis de status | OTP [8:10] | 89 ABCD | Fusíveis Programáveis (bytes) |
| 1 (8 bits) | Fusível MfrID | SN[8] | EE | Nunca zerou. |
| 4 (32 bits) | Fusível SN | SN[4:7] | 01 FC BF 7F | Bytes serão zeros dependendo do modo. |
| 2 (16 bits) | ROM MfrID | SN[0:1] | 01 23 | Nunca zerou. |
| 2 (16 bits) | ROM SN | SN[2:3] | 50 7B | Os bytes serão zeros dependendo do modo. |

2. Histórico de revisão

| Doc. Rev. | Data | Comentários |
|-----------|---------|---------------------------------|
| 8864A | 03/2013 | Liberação inicial do documento. |



Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 EUA

T: (+1)(408) 441.0311

F: (+1)(408) 436.4200

www.atmel.com

© 2013 Atmel Corporation. Todos os direitos reservados. / Rev.: Atmel-8864A-CryptoAuth-Migrating-AT88SA102S-ATSHA204-ApplicationNote-022013

Atmel®, o logotipo da Atmel e suas combinações, Enabling Unlimited Possibilities® e outros são marcas registradas ou marcas comerciais da Atmel Corporation ou de suas subsidiárias. 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 da Atmel. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, para qualquer direito de propriedade intelectual 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 SEUS PRODUTOS, INCLUINDO, SEM LIMITAÇÃO, A GARANTIA IMPLÍCITA DE COMERCIALIZABILIDADE, 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 USO ESTE DOCUMENTO, MESMO QUE A ATMEL TENHA 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 especificações 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 da Atmel não são destinados, autorizados ou garantidos para uso como componentes em aplicações destinadas a dar suporte ou sustentar a vida.