NOTA DE APLICAÇÃO

Troca de chave de criptografia de sessão simétrica

NOVO 204A

Introdução

Muitos sistemas precisam comunicar informações confidenciais por canais abertos. Os exemplos incluem controladores de semáforos onde as atualizações de firmware ocorrem pelo ar, redes de distribuição de energia onde as informações de consumo e/ou cobrança são transmitidas por linhas de energia e telemetria onde os dados do paciente são transmitidos por redes de telefonia móvel. A comunicação segura de informações confidenciais exige que o sistema de transmissão verifique a identidade do destinatário (autenticação) e embaralhe as informações para que outras pessoas não as vejam (criptografia).
A criptografia permite que ambas as tarefas sejam realizadas. Mas, embora muitos sistemas sejam capazes de executar os processos criptográficos subjacentes, eles não têm a capacidade de compartilhar com segurança as chaves criptográficas necessárias para estabelecer canais de comunicação confiáveis.

Um método alternativo para troca de chaves, como ECDH (Curva Elíptica Diffie-Hellman), pode ser facilmente implementado usando o Atmel® Dispositivo criptográfico CryptoAuthentication™ ATECC508A e é descrito em uma nota de aplicação diferente. A metodologia aqui descrita utiliza técnicas simétricas e pode ser implementada em dispositivos ATSHA204A, que podem ser mais atrativos para determinados sistemas. Observe que outros elementos de criptografia CryptoAuthentication, ou seja, o ATECC108A e o ATECC508A, são superconjuntos do ATSHA204A e também podem executar a metodologia descrita neste documento.

Este documento explica como os dispositivos de elemento criptográfico estabelecem uma raiz de confiança a partir da qual os sistemas podem gerar chaves de criptografia de sessão em uma extremidade e recuperá-las na outra sem realmente transmitir as chaves.

1 **Estabelecendo a raiz da confiança** A raiz da

confiança é o conhecimento secreto compartilhado que pode servir como base para transações confiáveis. Transações confiáveis incluem autenticação segura e comunicação confidencial de informações confidenciais. O conhecimento do segredo compartilhado geralmente está na forma de uma chave raiz da qual derivam as chaves de transação segura. O dispositivo criptográfico oferece a capacidade de incorporar chaves raiz não legíveis e não modificáveis de maneira a estabelecer a raiz de confiança.

Os dispositivos Atmel CryptoAuthentication™ são dispositivos de segurança invioláveis. Além de ter um True Random Number Generator (TRNG) e proteção de hardware contra adulteração física e ambiental, os dispositivos de criptografia implementam na lógica de hardware segura o algoritmo SHA-256, o algoritmo criptográfico mais robusto endossado por especialistas até o momento. Dos muitos recursos, a capacidade dos dispositivos criptográficos de armazenar segredos com segurança, gerar números aleatórios verdadeiros e executar hashes criptográficos SHA-256 permite que os sistemas comuniquem informações confidenciais com segurança em canais abertos. Ele faz isso gerando chaves de criptografia de sessão em um sistema e recuperando as mesmas chaves em outro sem realmente transmitir as chaves. Isso elimina completamente as chaves do reino de ataques no canal de comunicação.

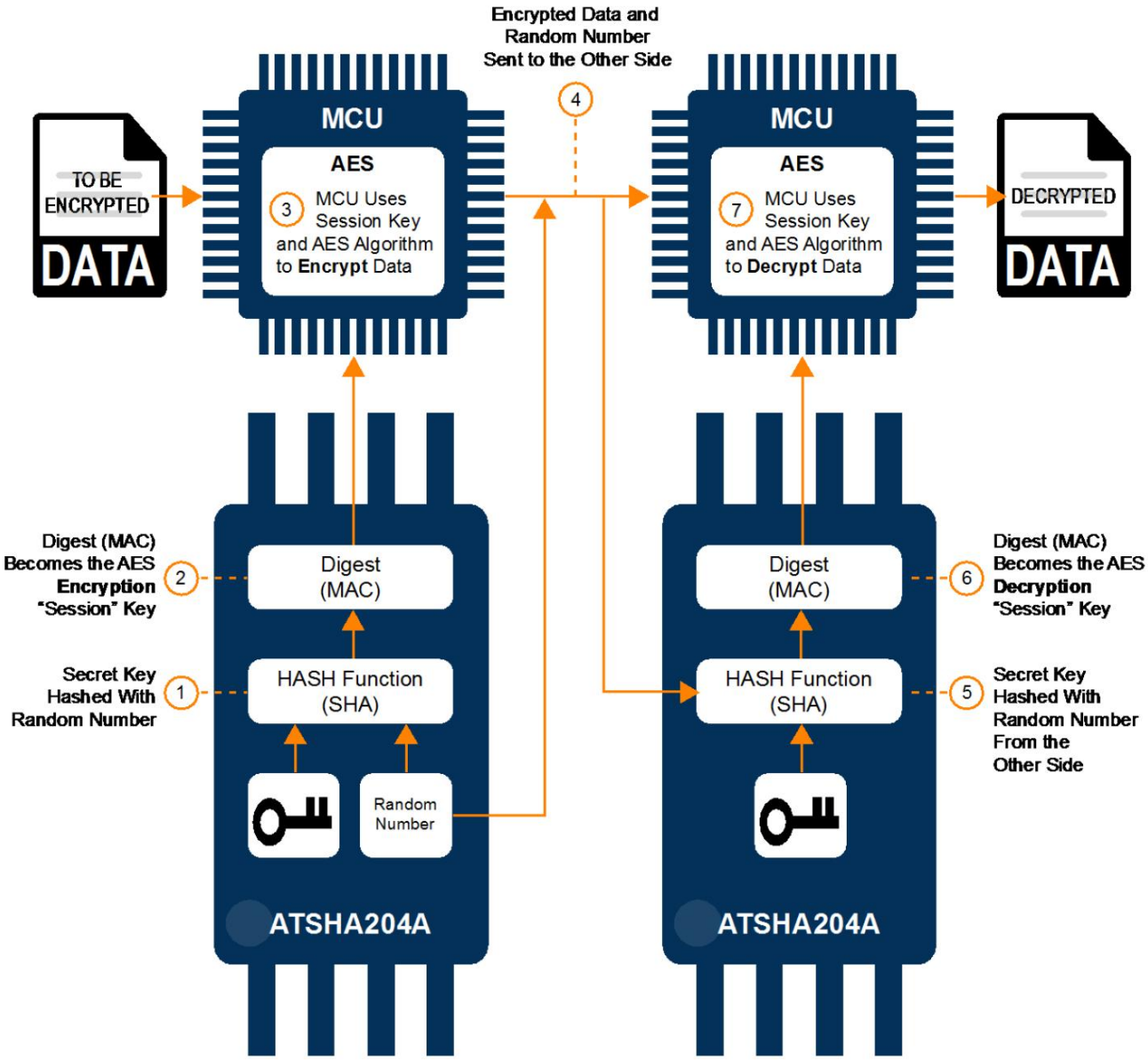
2 Geração, recuperação e segurança da chave de criptografia de sessão Comunicação

Tudo o que é necessário para gerar e recuperar chaves de criptografia de sessão entre dois ou mais sistemas de comunicação segura sem realmente transmitir as referidas chaves é um dispositivo criptográfico em cada sistema. Por meio de um processo chamado personalização do dispositivo, o integrador do sistema consegue incorporar segredos compartilhados personalizados em cada dispositivo criptográfico e usar mecanismos de segurança de hardware oferecidos pelo dispositivo para selar permanentemente os segredos da observação e/ou modificação. Cada segredo compartilhado oferece uma raiz única de confiança entre os sistemas.

Os sistemas normalmente requerem apenas uma raiz de confiança, mas ter várias pode oferecer a capacidade de diferenciar entre vários serviços. Por exemplo, um integrador de sistema pode optar por usar chaves raiz diferentes para comunicar o consumo de energia e as informações de faturamento em uma rede de distribuição de energia para acomodar as necessidades dos respectivos departamentos de manutenção em uma empresa de distribuição de energia.

Depois que os dispositivos estão nos sistemas, são necessárias várias etapas para realizar uma comunicação segura de ponta a ponta entre dois ou mais sistemas. As seções a seguir explicam essas etapas com mais detalhes e a figura a seguir ilustra como elas se encaixam.

Figura 2-1. Troca de chave de sessão



O dispositivo de elemento criptográfico ATSHA204A pode ser facilmente usado para troca segura de chaves de sessão. O elemento criptográfico funciona em conjunto com um MCU que realiza criptografia/descriptografia com um algoritmo como o AES. Para criar uma sessão de criptografia-descriptografia, o MCU de cada lado precisará de uma chave de criptografia-descriptografia idêntica. Para aumentar a segurança, a chave de cada lado deve mudar a cada sessão. É por isso que essas chaves são chamadas de chaves de sessão. A chave de sessão é trocada com segurança de um lado para o outro. Um número aleatório é usado para garantir que as chaves sejam diferentes para cada sessão.

Passo 1	Chave secreta hash com número aleatório

O processo começa com o hash da chave secreta armazenada no dispositivo ATSHA204A com um número aleatório criado pelo ATSHA204A. Observe que o sistema pode injetar o número aleatório no dispositivo criptográfico, mas a Atmel aconselha o uso do TRNG interno do dispositivo criptográfico para obter números aleatórios de alta qualidade para obter as chaves de criptografia de sessão mais eficazes. As chaves de criptografia de sessão eficazes são aquelas que praticamente nunca se repetem, evitando assim replay e ataques estatísticos. Este dispositivo também emitirá o número aleatório para uso posterior. A geração da chave de criptografia de sessão essencialmente abre uma sessão de comunicação confiável. A combinação do dispositivo criptográfico TRNG e as propriedades de entropia do algoritmo criptográfico SHA-256 garantem a qualidade das chaves de sessão.

Passo 2	Digest (MAC) torna-se chave de "sessão" de criptografia AES

O resultado da operação de hash será um código de autenticação de mensagem (MAC) de 32 bytes. 16 bytes desse MAC de 32 bytes (256 bits) de ATSHA204A serão a chave de sessão AES enviada para o MCU.

etapa 3	MCU usa a chave de sessão e AES para criptografar dados

O MCU executa um algoritmo de criptografia, como o Algoritmo AES, sobre os dados a serem criptografados.

Passo 4	Dados criptografados e número aleatório enviados para o outro lado

Os dados recém-criptografados e o número aleatório são enviados para o outro lado para que os dados possam ser descriptografados.

Passo 5	Digest (MAC) torna-se a chave de "sessão" de descriptografia AES

Para descriptografar a mensagem, a mesma chave usada para criptografá-la deve ser usada no processo de descriptografia. É exatamente por isso que o número aleatório é enviado, que é para recriar a chave de sessão desse número aleatório e a chave armazenada no ATSHA204A no lado da descriptografia. Isso é feito pelo número aleatório inserido no algoritmo de hash SHA-256 junto com a chave armazenada no ATSHA204A. Como esta é uma operação simétrica, as chaves secretas armazenadas nos dispositivos ATSHA204A em ambos os lados são idênticas. Quando o mesmo número aleatório é hash com a mesma chave secreta, o resumo de 32 bytes resultante será o mesmo no lado do receptor (descriptografia) e no lado do remetente (criptografia).

Passo 6	Chave secreta hash com número aleatório do outro lado

Assim como o lado da criptografia, 16 bytes do resumo (ou seja, MAC) representam a chave de criptografia/descriptografia e são inseridos no MCU.

Passo 7	MCU usa chave de sessão e algoritmo AES para descriptografar dados

O MCU do lado receptor executa o algoritmo de descriptografia (como AES) usando a chave de sessão para descriptografar o código criptografado que foi enviado do outro lado. A disposição das chaves de criptografia da sessão, juntamente com a disposição anterior dos números aleatórios pelos sistemas inicial e receptor, encerra essencialmente a sessão confiável. Em outras palavras, não existe mais informação suficiente para recuperar ou reproduzir essa sessão, desde que o número aleatório usado seja de uma fonte de qualidade como o TRNG do dispositivo criptográfico. Ao controlar a frequência com que uma chave de sessão é gerada no sistema iniciador, o integrador de sistema controla efetivamente o tempo de vida da sessão determinado pelo número de transações seguras, ou seja, transmissão e recuperação de dados confidenciais.

3 Autenticação de ponta a ponta

Os requisitos necessários para sistemas de comunicação segura são a capacidade de autenticar destinatários e criptografar informações confidenciais. O uso de um dispositivo de elemento criptográfico realiza ambos. Embora a satisfação do requisito de criptografia agora seja evidente, o mesmo pode não ser aparente para a autenticação. Somente um dispositivo criptográfico personalizado de forma idêntica pode recuperar a chave de criptografia da sessão, e apenas sistemas autênticos estarão de posse de tais dispositivos personalizados. A recuperação bem-sucedida da chave de criptografia da sessão prova essencialmente a autenticidade mútua dos sistemas inicial e de destino. Um sistema não autêntico não poderá recuperar a chave de criptografia da sessão e, portanto, não poderá obter acesso às informações confidenciais. Em outras palavras, apenas sistemas mutuamente autênticos podem se comunicar com segurança, e a autenticação efetivamente deriva do segredo raiz compartilhado dentro dos limites fortificados do dispositivo de elemento criptográfico (ou seja, nos mecanismos de armazenamento de chaves seguras).

4 Comandos de Interesse

Os dispositivos de elemento criptográfico da Atmel vêm com um rico conjunto de comandos que oferecem aos integradores de sistema alta flexibilidade para lidar com vários desafios de segurança. Após a personalização do dispositivo, apenas três desses comandos são necessários para realizar a aplicação descrita neste documento. Eles são os comandos Random, MAC e Nonce, descritos na tabela a seguir.

Tabela 4-1. **Comandos de CriptoAutenticação de Interesse**

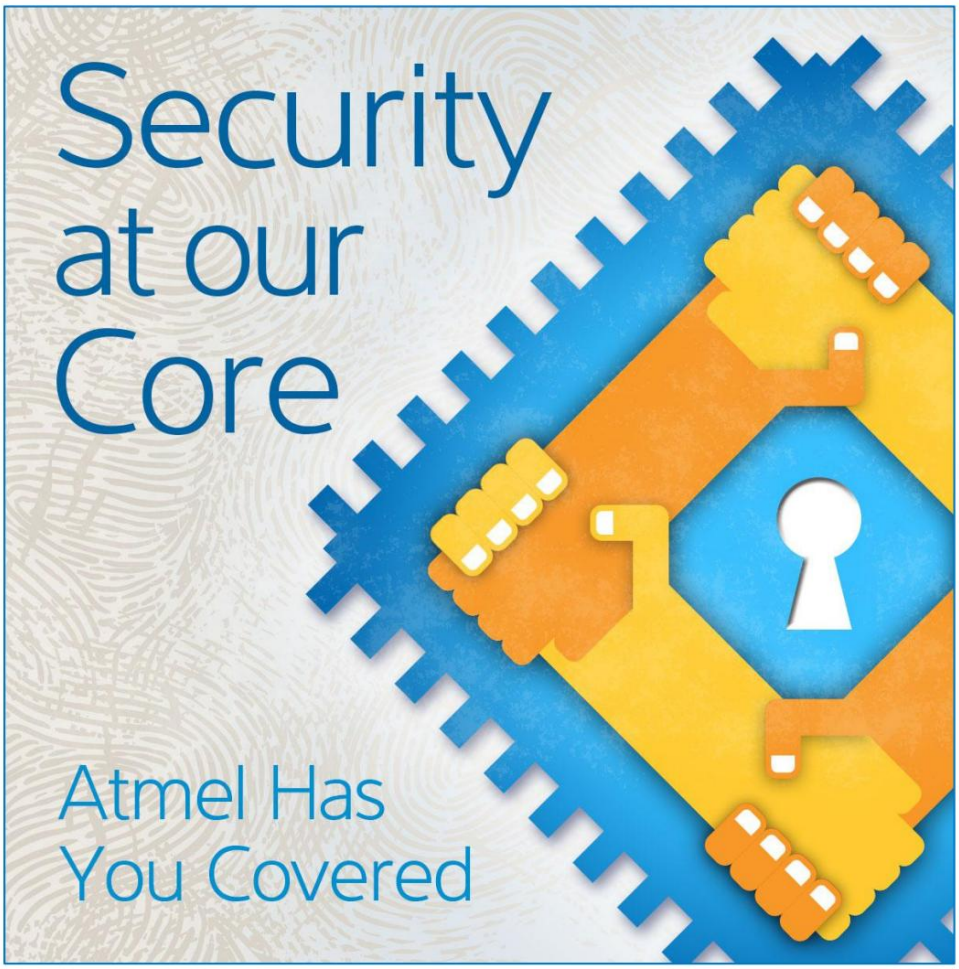
Descrição do comando	
aleatório	Gera um número aleatório para a criação de chaves de criptografia de sessão.
MAC	Combina o número aleatório com o segredo raiz incorporado para criar ou recuperar a chave de criptografia da sessão.
Nonce	Um precursor do comando MAC cuja função é inicializar o dispositivo criptográfico em um estado interno de alta entropia. Alta entropia neste contexto é desejável porque elimina a facilidade de adivinhar e montar ataques de repetição. Essa lista minúscula de comandos enfatiza a facilidade de implementação e a demanda mínima de recursos do sistema, como largura de banda da CPU e requisitos de armazenamento de código.

4. Conclusão

Entre seus inúmeros recursos, a família de produtos CryptoAuthentication oferece uma abordagem econômica para sistemas de comunicação para troca segura de chaves de criptografia de sessão em canais abertos sem realmente transmitir as próprias chaves. Ele faz isso estabelecendo uma raiz de confiança entre os sistemas de comunicação e permitindo que um sistema inicial gere chaves de criptografia de sessão que são recuperáveis apenas por sistemas receptores autênticos. O mesmo dispositivo também estabelece a autenticidade mútua dos sistemas de comunicação.
Os dispositivos oferecem facilidade de implementação com comandos de alto nível e exigem muito pouco em termos de sistema recursos.

5 Histórico de Revisão

Doutor Rev.	Data	Comentários
8777B	11/2015	A nota do aplicativo, o modelo e os dispositivos CryptoAuthentication foram atualizados.
8777A	06/2011	Liberação inicial do documento.



Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 **www.atmel.com**