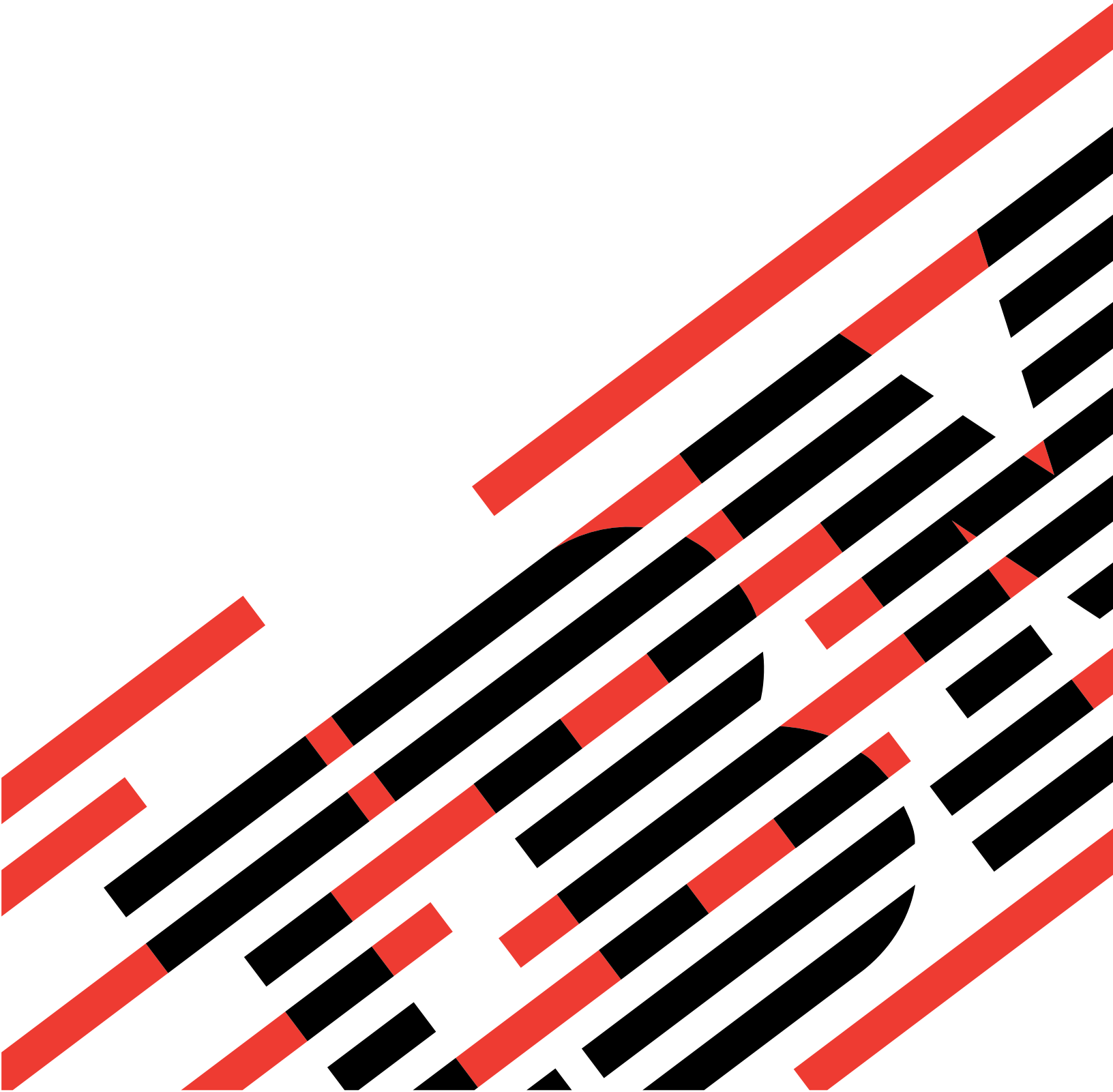
IBM

eserver

iSeries

暗号化ハードウェア



IBM

@server

iSeries

暗号化ハードウェア

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原　典： RZAJ–C000–04
iSeries
Cryptographic hardware

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2002.11

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 1998, 2003. All rights reserved.

© Copyright IBM Japan 2002

目次

© Copyright IBM Corp. 1998, 2003

第 1 部 2058 暗号化アクセラレーター

© Copyright IBM Corp. 1998, 2003

第 1 章 トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。

- 『暗号化ハードウェア』(約 1322 KB、298 ページ)。ここには、iSeries™ V5R2 サーバー用にサポートされている、IBM® 暗号化ハードウェアに関するすべての情報が記載されています。
- 『暗号化ハードウェア: 2058 暗号化アクセラレーター』(約 355 KB、24 ページ)。ここには、iSeries V5R2 サーバー用にサポートされている、2058 暗号化アクセラレーター・ハードウェアに関する情報が記載されています。

PDF ファイルの保管

表示用または印刷用の PDF ファイルを Netscape Navigator からワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタンでクリックする。
2. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) をクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Acrobat Reader のダウンロード

PDF ファイルを表示したり印刷したりするには、Adobe Acrobat Reader が必要です。これは、Adobe Web サイト  からダウンロードできます。

© Copyright IBM Corp. 1998, 2003

第 2 章 V5R2 の新機能

新しい暗号化ハードウェアに関する最新情報、および iSeries サーバー用の既存の暗号化ハードウェア・オプションに追加されたフィーチャーに関する最新情報については、このトピックを参照してください。

»

新しい暗号化ハードウェア: IBM 2058 e-business 暗号化アクセラレーター

4758 暗号化コプロセッサーに加えて、IBM 2058 e-business 暗号化アクセラレーター (ハードウェア・フィーチャー・コード 4805、これ以後は 2058 暗号化アクセラレーターと記述します) が使用可能です。秘密鍵の処理をシステム・プロセッサーの外部に転送することで、iSeries のパフォーマンスを向上させる設計となっており、大量の SSL (Secure Sockets Layer) トランザクションを処理するため、iSeries のインプリメンテーションにおいて、このハードウェア・オプションは優れた選択肢です。2058 暗号化アクセラレーターは、iSeries サーバーの SSL パフォーマンスを向上させるための優れた選択肢ではありますが、4758 コプロセッサーが提供するような広範囲の構成オプションは提供しません。

ご使用の iSeries サーバーのインプリメンテーションにはどちらの暗号化ハードウェア・オプションが最適であるかを判断する際に参考となる詳細情報については、『2058 暗号化アクセラレーター』を参照してください。

追加機能: 4758 暗号化コプロセッサー

4758 暗号化コプロセッサーは、以下の新しい機能を提供します。

- 金融サービスにおける PIN 処理: トランザクションごとの固有キー (UKPT)
- Common Cryptographic Architecture (CCA) 2.4

新しい暗号化ハードウェアのシナリオ

暗号化ハードウェアを iSeries サーバーでどのように使用できるかについて例示するために、以下のシナリオを iSeries Information Center に追加しました。

- 『暗号化ハードウェアのシナリオ: iSeries SSL のパフォーマンスの向上』

このリリースでの新機能または変更点についてのその他の情報は、「プログラム資料説明書」

を参照してください。«

新機能または変更箇所の見分け方

技術上の変更が行なわれた箇所を見分ける上で役立つように、この情報では以下の記号を使用しています。

- » のイメージは、新しい情報または変更された情報の始まりを示しています。

© Copyright IBM Corp. 1998, 2003

-  のイメージは、新しい情報または変更された情報の終わりを示しています。

第 3 章 概念

暗号

暗号は、データを安全に保持するための技術です。基本的な暗号化サービスにより、メッセージがプライベートなものであること、メッセージの保全性が保持されること、通信している当事者が認証されていること、および通信に関与している一方の当事者がメッセージの送信を拒否できないことが保証されます。

暗号を使用すると、保管されたデータまたは通信を、関係のない第三者が理解できないようにしながら、情報を保管したり他の人と通信することができます。暗号化は、理解可能なテキストを理解不能なデータ部分 (暗号文) に変換します。暗号化解除は、理解不能なデータから理解可能なテキストを復元します。両方のプロセスには、数学の公式またはアルゴリズム、および秘密データ (キー) がかかわっています。

暗号アルゴリズム

暗号アルゴリズムには、以下の 2 つのタイプがあります。

1. 秘密鍵アルゴリズム、つまり**対称鍵アルゴリズム**では、1 つのキーが、通信する 2 つの当事者間で共用秘密鍵になります。暗号化および暗号化解除の両方に、同じキーを使用します。秘密鍵アルゴリズムの例としては、データ暗号化規格 (DES) および Triple-DES があります。
2. 公開鍵アルゴリズム、つまり**非対称鍵アルゴリズム**では、キーのペアが使用されます。一方のキーである秘密鍵は秘密にされ、誰とも共用されません。もう一方のキーである公開鍵は秘密ではなく、他人と共用されます。これらのキーのどちらか一方でデータが暗号化されると、そのデータはもう一方のキーでしか暗号を解除して復元することができません。この 2 つのキーは数学的に関連していますが、秘密鍵を公開鍵から派生させることは事実上不可能です。公開鍵アルゴリズムの例としては、RSA アルゴリズムがあります。

どちらのタイプのアルゴリズムでも、データの変更方法を判断するためにキーを使用します。さまざまな暗号プロセスは、いくつかの目的のうちの 1 つを達成するために 1 つのアルゴリズムを使用しています。メッセージ確認コード (MAC) を生成してデータの保全性を保証する場合のように、目的によって使用する暗号化プロセスを選択します。 4758 暗号化コプロセッサー用のユーザー作成アプリケーションは、対応するセキュリティー・アプリケーション・プログラミング・インターフェース (SAPI) を使用して暗号プロセスを呼び出します。キーと暗号プロセスが一緒になってデータを変換します。 SAPI の権限を持つユーザーは、その暗号プロセスにアクセスすることができます。したがって、キーはデータへのアクセスを制御します。データを保護するには、キーを保護する必要があります。キー値を秘密にしておけば、そのキーでアルゴリズムを使用することにより、データのセキュリティーを保証することができます。

暗号化

© Copyright IBM Corp. 1998, 2003

ユーザー・アプリケーションは、フィールド・レベルの暗号化を使用して、明示的に暗号サービスを要求します。ユーザー・アプリケーションは、キーの生成、選択および分配を完全に制御します。ユーザー・アプリケーションは、暗号化するデータおよび非暗号化テキストとして保管するデータも制御します。システムは、セッション層での暗号化を使用して、アプリケーションに代わって暗号サービスを要求します。アプリケーションが、暗号化が行われていることを認識している場合も、していない場合もあります。リンク・レベルの暗号化は、プロトコル・スタックの最下層で実行されますが、通常、リンク・レベルの暗号化のための専用のハードウェアで実行されます。4758 コプロセッサーは、フィールド・レベルの暗号化と、SSL (Secure Sockets Layer) のセッション確立のための暗号化の両方をサポートしていますが、VPN および SNA のセッション・レベルでの暗号化はサポートしていません。2058 暗号化アクセラレーターは、SSL のセッション確立のための暗号化のみをサポートしています。

データ保全性

データを信頼するためには、データが許可された送信元から送られていて、かつ変更されていないことを知る必要があります。これは、データ認証性およびデータ保全性と呼ばれます。 4758 コプロセッサーは、メッセージ確認コード (MAC)、メッセージ要約、あるいはディジタル署名を作成することにより、認証性と保全性を保証しています。

メッセージ確認コード (MAC)

MAC プロセスは、重要なデータ要素を定義するデータ保全のための技法です。たとえば、資金転送メッセージで金額を定義することができます。 MAC は、重要なデータ要素、暗号アルゴリズム、および機密 MAC キーから構成されます。 MAC は、メッセージの一部になり、メッセージと共に送信されます。MAC プロセスは DES キーまたは Triple-DES キーを使用します。

メッセージの受信側は、送信側と同じ MAC キー、アルゴリズム、およびプロシージャーを使用して MAC を複製します。受信側の MAC がメッセージと一緒に送られた MAC と一致すると、変更されていないものとして MAC を受け入れることができます。

MAC プロセスでは、受信したメッセージを認証できるようになりますが、転送データは非暗号化テキストのままなので許可なしに読み取られます。 MAC プロセスを使用し、さらにメッセージ全体を暗号化すると、データのプライバシーと保全性を効率的に保護することができます。

メッセージ要約

メッセージ要約のプロセスをデータに対して実行すると、暗号的に生成されたチェックサムと見なされる要約値を作成することができます。データの一部が変更された場合は、異なる要約が生成されます。メッセージ要約のコピーを保持しておき、それらを比較することができます。メッセージ要約が等しいということは、データが変更されていないことを示します。

ディジタル署名

ディジタル署名も、認証性と保全性を検証するために使用できます。これは、以下の 2 ステップから成るプロセスです。

1. 最初にダイジェストがデータから生成され、次にそのダイジェストが RSA 秘密鍵を使用して暗号化されます。この結果がディジタル署名になります。ディジタル署名は、公開鍵を使用してその署名を暗号解除し、オリジナルのダイジェストを回復することにより検証することができます。
2. もう 1 つのダイジェストは、データから生成され、オリジナルのダイジェストと比較されます。この 2 つが同一であれば、その署名は証明されたことになり、データが変更されていないことを確認することができます。

4758 暗号化コプロセッサーに関連するキーのタイプ

4758 コプロセッサーはさまざまなキーのタイプを使用します。すべての対称鍵操作に対して、すべての DES キーあるいは Triple-DES キーを使用できるわけではありません。同様に、すべての非対称鍵操作に対して、すべての公開鍵アルゴリズム (PKA) キーを使用できるわけではありません。4758 コプロセッサーが使用する各種キー・タイプのリストを以下に示します。

マスター・キー

このキーはクリア・キーで、他のキーが暗号化されていないことを意味します。4758 コプロセッサーは、マスター・キーを使用してすべての操作キーを暗号化します。4758 コプロセッサーは、マスター・キーを改ざんされにくいモジュールに保管します。このマスター・キーは、4758 コプロセッサーからは取り出すことはできません。4758 コプロセッサーは、改ざんに対しては、マスター・キーとその工場認証を破棄することにより対応します。4758-023 は、DES キーの暗号化用と PKA キーの暗号化用にそれぞれ 1 つずつの、2 つのマスター・キーを持っています。

倍長鍵暗号鍵

4758 コプロセッサーは、このタイプの Triple-DES キーを使用して他の DES キーまたは Triple-DES キーを暗号化、または暗号化解除します。鍵暗号鍵は、通常、システム間でキーを転送するために使用されます。ただし、バックアップ用に、オフラインでキーを保管するために使用することもできます。鍵暗号鍵をキーの転送に使用する場合は、鍵暗号鍵自体のクリア値を 2 つのシステム間で共用しなければなりません。エクスポーターの鍵暗号鍵は、エクスポート操作に使用されます。エクスポート操作では、マスター・キーで暗号化されたキーは、暗号化解除され、次に鍵暗号鍵で暗号化されます。インポーターの鍵暗号鍵は、インポート操作に使用されます。インポート操作では、鍵暗号鍵で暗号化されたキーは、暗号化解除され、次にマスター・キーで暗号化されます。

倍長 PIN キー

4758 コプロセッサーはこのタイプのキーを使用して、金融操作で使用される PIN を生成、検証、暗号化、および暗号化解除を行います。これらのキーは Triple-DES キーです。

MAC キー

4758 コプロセッサーは、このタイプのキーを使用して、メッセージ確認コード (MAC) を生成します。これらのキーは、DES キーまたは Triple-DES キーのいずれかです。

暗号鍵 4758 コプロセッサーは、このタイプのキーを使用して、データの暗号化または暗号解除を行います。これらのキーは、DES キーまたは Triple-DES キーのいずれかです。

単一長互換性キー
4758 コプロセッサーは、このタイプのキーを使用してデータの暗号化または暗号化解除を行い、さらに MAC を生成します。これらのキーは DES キーであり、 Common Cryptographic Architecture をインプリメントしていないシステム間で、暗号化されたデータまたは MAC を交換する場合によく使用されます。

秘密鍵 4758 コプロセッサーは、ディジタル証明書の生成、および公開鍵で暗号化された DES キーまたは Triple-DES キーの暗号化解除に秘密鍵を使用します。

公開鍵 4758 コプロセッサーは、ディジタル署名の妥当性検査、DES キーまたは Triple-DES キーの暗号化、および秘密鍵で暗号化されたデータの暗号化解除に公開鍵を使用します。

キー形式

4758 コプロセッサーは、4 つの異なる形式のうちいずれか 1 つで、キーを操作します。キー形式は、キー・タイプと一緒になって、暗号プロセスがそのキーを使用する方法を決定します。以下に 4 つの形式を示します。

クリア形式
キーのクリア値は、どの暗号手段によっても保護されません。クリア・キーは、4758 コプロセッサーでは使用できません。クリア・キーは、最初にセキュア・モジュールにインポートして、マスター・キーで暗号化し、次にセキュア・モジュールの外部に保管しなければなりません。

操作可能形式
マスター・キーで暗号化されたキーの形式は、操作可能形式です。これらのキーは、4758 コプロセッサーでは暗号操作に直接使用できます。操作キーは、内部キーとも呼ばれます。サーバーの鍵ストア・ファイルに保管されているキーはすべて操作キーです。しかし、すべての操作キーを鍵ストア・ファイルに保管する必要はありません。

エクスポート形式
エクスポート操作の結果、エクスポーターの鍵暗号鍵で暗号化されたキーの形式は、エクスポート形式です。これらのキーは外部キーとも呼ばれます。エクスポート形式のキーは、エクスポーターの鍵暗号鍵と同じクリア・キー値を持つインポーターの鍵暗号鍵が存在している場合は、インポート形式であると記述することもできます。キーは、任意の方法で、エクスポート形式で保管することができますが、鍵ストア・ファイルに保管することはできません。

インポート形式
インポーターの鍵暗号鍵で暗号化されたキーの形式は、インポート形式です。インポート操作にソースとして使用できるのは、インポート形式のキーのみです。これらのキーは外部キーとも呼ばれます。インポート形式のキーは、インポーターの鍵暗号鍵と同じクリ

ア・キー値を持つエクスポーターの鍵暗号鍵が存在している場合は、エクスポート形式であると記述することもできます。キーは、任意の方法で、インポート形式で保管することができますが、鍵ストア・ファイルに保管することはできません。

機能制御ベクトル

IBM は、機能制御ベクトルとして知られる、ディジタル署名された値を提供しています。この値を使用すると、4758 コプロセッサー内の暗号アプリケーションは、適用可能なインポート制限とエクスポート制限に一致するレベルの暗号サービスを提供することができます。機能制御ベクトルは、システムに導入される IBM Cryptographic Access Provider (5769-ACx) 製品に付属しています。ファイルのパス名は、/QIBM/ProdData/CAP/FCV.CRT です。機能制御ベクトルを使用すると、4758 コプロセッサーにキーの作成に必要なキー長の情報を得ることができます。

制御ベクトル

制御ベクトルは、機能制御ベクトルとは異なり、以下を制御するキーに関連付けられた既知の値です。

- キーの型
- このキーが暗号化できる他のキーの種類
- ユーザーの 4758 コプロセッサーがこのキーをエクスポートできるかどうか
- このキーに対して許可された他の使用

制御ベクトルは暗号を介してキーにリンクしているため、制御ベクトルを変更する場合は、同時にキーの値も変更しなければなりません。

鍵ストア・ファイル

4758 コプロセッサーのマスター・キーで暗号化されたキーを保管するために使用される、OS/400® データベース・ファイルです。

キー・トークン

暗号キー、制御ベクトルおよびキーに関連するその他の情報を持つことができるデータ構造。キー・トークンは、キーに作用する、あるいはキーを使用するほとんどの CCA API のパラメーターとして使用されます。

第 4 章 2058 暗号化アクセラレーター

2058 暗号化アクセラレーターは、V5R2 (以降) の iSeries サーバーで使用可能です。2058 暗号化アクセラレーターは、4758 暗号化コプロセッサーほどのハイ・セキュリティーは必要としないものの、ホスト・プロセッサーの負荷を軽減するために、ハードウェアによるアクセラレーションが提供する、パフォーマンスの高い暗号化を必要とするユーザーに対し、競争力のあるオプションを提供します。2058 暗号化アクセラレーターは、キーのセキュアな保管場所を必要としない SSL アプリケーションのパフォーマンスを向上させるように設計されています。2058 暗号化アクセラレーターでは、4758 暗号化コプロセッサーのような、改ざんされにくいキーの保管場所は提供されません。1 つの iSeries サーバーに最大 4 つの 2058 暗号化アクセラレーター・カードをインストールできます。

2058 暗号化アクセラレーターは、RSA 暗号化 (モジュラー指数) 用に最適化された、最大 2048 ビットのデータ・キー長を持つ、特殊なハードウェアを提供します。2058 アクセラレーターは、複数の RSA (Rivest、Shamir、および Adleman アルゴリズム) エンジンを使用します。ご使用の iSeries サーバー・モデルに特有のパフォーマンス情報については、『iSeries Performance Management』 Web サイトを参照してください。

2058 暗号化アクセラレーターについての詳細は、以下のページを参照してください。

- 『2058 暗号化アクセラレーターのフィーチャー』
- 『暗号化ハードウェアのシナリオ: iSeries SSL のパフォーマンスの向上』
- 『2058 暗号化アクセラレーターの計画』
- 『2058 暗号化アクセラレーターの構成』

2058 暗号化アクセラレーターのフィーチャー

2058 暗号化アクセラレーターのフィーチャーには、以下のようなものがあります。

- 単一カードのハイパフォーマンス暗号化アダプター (標準 PCI カード)
- RSA 暗号化用の設計および最適化
- オンボード・ハードウェア・ベースの RNG (乱数発生ルーチン)
- IBM UltraCypher 暗号エンジンを 5 つ搭載

以下の 2058 暗号化アクセラレーターに関する情報を参照してください。

- 『2058 暗号化アクセラレーターの計画』
- 『2058 暗号化アクセラレーターの構成』

© Copyright IBM Corp. 1998, 2003

暗号化ハードウェアのシナリオ: iSeries SSL のパフォーマンスの向上

この暗号化ハードウェアを iSeries サーバーと共にどのように使用できるかという一例を示すために、以下の使用例のシナリオを追加しました。

状況

ある会社の iSeries サーバーが、1 日当たり数千のセキュア・インターネット・トランザクションを処理しているとします。その会社のトランザクションでは、SSL (Secure Sockets Layer) および Transport Layer Security のプロトコル (SSL および TLS、インターネット・トランザクションを保護するための一般的な方式) を使用しています。この会社のシステム管理者である Sue は、追加のアプリケーション・プロセスを行うために (さらに多くの SSL トランザクションをサポートできるようにすることも含む)、サーバー資源を解放したいと考えています。Sue は、以下の目標を達成できるソリューションを探しています。

- アプリケーション・プロセス (追加の SSL トランザクションも含めて) で使用可能なサーバー資源のサイズを大幅に増やすことができる
- インストールおよび構成の作業が最小限に抑えられる
- 資源管理の必要が最低限に抑えられる

これらの目標に基づいて、Sue は IBM 2058 e-business 暗号化アクセラレーターを注文し、インストールします。(これ以後は、2058 暗号化アクセラレーターと記述します。) 2058 暗号化アクセラレーターは PCI カードで、SSL/TLS セッションの確立の際に必要となる、極めて計算中心の処理を高速化するように、特別に設計されています。iSeries サーバーでは、ハードウェア・フィーチャー・コード 4805 を注文すると、2058 暗号化アクセラレーターが入手できます。

詳細

1. iSeries サーバーに 2058 暗号化アクセラレーターがインストールされ、構成されています。
2. iSeries サーバーが、ネットワークから大量の SSL トランザクション要求を受信します。
3. 2058 暗号化アクセラレーターが、SSL トランザクションの開始時に暗号処理を実行し、SSL トランザクションのディジタル証明書に関連付けられている秘密鍵をキャッシュに入れます。

前提条件および前提事項

このシナリオでは、Sue が 2058 暗号化アクセラレーターのインストールを計画し、カードを正しく構成したことを前提としています (『2058 暗号化アクセラレーターの計画』および『2058 暗号化アクセラレーターの構成』を参照)。また、Sue が SSL のディジタル証明書のセットアップをすでに完了していることも前提となっています。

構成ステップ

Sue は、会社の iSeries サーバーの SSL のパフォーマンスを向上させるために、以下のステップを実行します。

1. 2058 暗号化アクセラレーターを提供する、ハードウェア・フィーチャー・コード 4805 を注文します。
2. 2058 暗号化アクセラレーターをインストールします。
3. 2058 暗号化アクセラレーターの装置記述を作成し、装置をオンに変更します (詳細については、『2058 暗号化アクセラレーターの構成』を参照)。

2058 暗号化アクセラレーターの計画

2058 暗号化アクセラレーターをインストールして使用する前に、サーバーが以下の要件を満たしている必要があります。

ハードウェア要件

IBM e-business 暗号化アクセラレーター (注文可能なフィーチャー・コード 4805、これ以後は 2058 暗号化アクセラレーターと記述します)。 4805 フィーチャーは標準 PCI カードであり、以下の iSeries サーバー・モデルでサポートされます。

- 270
- 810、820、825、830、840、870 および 890
- SB2 および SB3
- 拡張装置 5074、5075、5078、5079、5088、5094、5095 および 5294

OS/400 および SSL の要件

2058 暗号化アクセラレーターでは、OS/400 V5R2M0 (バージョン 5 リリース 2 モディフィケーション 0) のソフトウェアが必要です。2058 暗号化アクセラレーターは暗号操作を完全に利用できるようになっていますが、SSL も使用する OS/400 で暗号機能を使用可能にするには、iSeries サーバー上に Cryptographic Access Provider 128-bit (5722-AC3) ライセンス・プログラム製品もインストールされていなければなりません。

2058 暗号化アクセラレーターの構成

装置記述を作成して、OS/400 SSL が RSA 暗号操作を 2058 暗号化アクセラレーターに送るようにしなければなりません。装置記述は、装置記述の作成 (暗号) (CRTDEVCRP) CL コマンドを使用して作成できます。

装置記述の作成

CL コマンドを使用して装置記述を作成するには、以下のステップを実行します。

1. コマンド行に CRTDEVCRP と入力します。
2. プロンプトが表示されたときに、装置の名前を指定します。
3. PKA 鍵ストア庫のデフォルト名 *NONE を受け入れます。
4. DES 鍵ストア庫のデフォルト名 *NONE を受け入れます。
5. プロンプトが表示されたら記述を指定します。この指定はオプションです。

6. 装置記述の作成が完了した後、構成変更 (VRYCFG) または構成状況処理 (WRKCFGSTS) CL コマンドを使用して、装置の構成を変更します。

ソフトウェアで生成され、ソフトウェアに保管されるディジタル証明書では、装置がオンになった後で、OS/400 SSL が自動的に 2058 暗号化アクセラレーターの使用を開始します。SSL および TLS のセッション確立に関連した秘密鍵の処理が 2058 暗号化アクセラレーターへオフロードされます。装置がオフになっている場合は、OS/400 SSL が、SSL および TLS のセッション確立のための暗号化を、ソフトウェア・ベースの暗号化にスイッチバックします。したがって、秘密鍵の処理がサーバーに戻されます。

注: これは、4758 暗号化コプロセッサー以外で作成された証明書および秘密鍵についてのみ当てはまります。証明書が、4758 暗号化コプロセッサーを使用して生成されたものである場合は、その特定の証明書を使用する SSL または TLS のセッションには、4758 暗号化コプロセッサーを使用しなければなりません。

『暗号化ハードウェアのシナリオ: iSeries SSL のパフォーマンスの向上』のページで、2058 暗号化アクセラレーターをインストールし、オンにした後での、iSeries サーバーにおける 2058 暗号化アクセラレーターの使用例のシナリオを示しています。 

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12