iAnywhere SOLUTIONS
A SYBASE COMPANY

WHITE PAPER

Mobile Link トランスポート・レイヤのセキュリティおよびデジタル証明書

概要

Mobile Link トランスポート・レイヤのセキュリティは、Mobile Link クライアントとMobileLink 同期サーバ間で転送される同期データ・ストリームの機密性および整合性を保護するものです。また、これにより、クライアント・アプリケーションがMobile Link 同期サーバの識別情報を検証し、信頼されたMobile Link 同期サーバだけと同期することができます。

このセキュリティはデジタル証明書を使用して実装するもので、デジタル証明書は必要なセキュリティ・レベルに応じてさまざまな方法で使用することができます。この本書では、公開鍵暗号化の基本概念と、デジタル証明書への応用方法について説明します。また、使用方法についても、いくつかの例をもとに解説します。

e-BUSINESS ANYWHERE

目次

セクション I：Mobile Link トランスポート・レイヤのセキュリティおよび証明書

Mobile Link トランスポート・レイヤのセキュリティは、Mobile Link クライアントと Mobile Link 同期サーバの間で転送される同期データ・ストリームの機密性および整合性を保護します。また、これにより、クライアント・アプリケーションが Mobile Link 同期サーバの識別情報を検証し、信頼された Mobile Link 同期サーバだけと同期することができます。このセキュリティは、デジタル証明書を使用して実装します。デジタル証明書は、必要なセキュリティ・レベルに応じてさまざまな方法で使用することができます。このホワイトペーパーでは、公開鍵暗号化の基本概念と、デジタル証明書への応用方法について説明し、いくつかの異なる使用方法を例示します。

セクション II：公開鍵暗号化について

公開鍵暗号化では、膨大な数値の組み合わせを処理する数学的な手法を利用します。これらの数値 (鍵と呼びます) には、特定の属性があります。一方の公開鍵と呼ばれる鍵は、公開の場 (電話帳など) で公開され、暗号化情報を公開鍵の所有者に送信することができます。公開鍵の所有者は、秘密鍵と呼ばれるもう一方の鍵を非公開にしておきます。

公開鍵で暗号化したメッセージは、秘密鍵を使用した場合にだけ復号化することができます。公開鍵は公開されているため、すべてのユーザが秘密鍵の所有者だけが読み取ることのできるメッセージを作成することができます。また、公開鍵を入手したユーザは、秘密鍵で暗号化されたメッセージを復号化することができます。これにより、秘密鍵の所有者は、対応する公開鍵で復号化可能なメッセージを秘密鍵を使用して作成することで、秘密鍵を所有していることを " 証明 " することができます。

公開鍵から秘密鍵を簡単に特定できないようにすることが必要です。公開鍵から秘密鍵を特定するのがどの程度困難かは、多くの場合は暗号化システムの強度および公開鍵のサイズ (ビット数) によって決まります。秘密鍵は、推測が困難であることも必要です。高品質の秘密鍵を生成するには、完全に予測不可能な乱数を使用する必要があります。Mobile Link で提供されるツールでは、新しい秘密鍵を生成する際に、オペレーティング・システムから疑似乱数データを収集します。このデータが予測可能であると、不正ユーザに鍵の値を予測される可能性があります。

セクション III：デジタル証明書について

デジタル証明書は、ユーザまたはエンティティを識別するための電子ドキュメントであり、そのユーザまたはエンティティの公開鍵のコピーが含まれています。証明書内の公開鍵を使用して、任意のユーザが情報を暗号化し、公開鍵を所有するユーザまたはエンティティとセキュアな通信を実行することができます。デジタル証明書は、以下の情報を含む規格化されたファイル・フォーマットに準拠しています。

1. 証明書の所有者の名前や住所などの識別情報

2. 公開鍵

3. 有効期限

4. 証明書の変更を防止するためのデジタル署名

デジタル署名

デジタル署名を使用して、証明書の変更を検出することができます。デジタル署名は、識別情報および公開鍵のメッセージ・ダイジェストと呼ばれる値を計算して作成する暗号化処理です。

メッセージ・ダイジェストは、証明書が変更されると変化するように設計された、計算によって生成するビット値です。メッセージ・ダイジェストの計算に使用するアルゴリズムは、すべての証明書ユーザに公開されています。正しい値は、証明書用の秘密鍵を使用して暗号化されます。すべての証明書のユーザがメッセージ・ダイジェストを計算できるため、変更を検出するには、メッセージ・ダイジェスト値を計算し、証明書に含まれたメッセージ・ダイジェスト値を公開鍵で復号化するだけです。2 つの値が異なる場合は、証明書が変更されています。

デジタル署名は対応する秘密鍵で作成されているため、この方法で作成した証明書を自己署名証明書と呼びます。このような証明書は、秘密鍵がないかぎり変更することはできません。

セクション IV：Mobile Link の同期での証明書の使用

Mobile Link 同期サーバでは、独自のサーバ証明書を使用してクライアントに識別情報を提供する必要があります。クライアントは証明書が本物であることを確認する必要があるため、サーバの公開証明書のコピーをクライアントがすでに入手しているか、クライアントが信頼する証明書によってサーバの証明書が署名されている必要があります。後者の場合は、署名済みの公開証明書の信頼できるコピーをクライアントが入手している必要があります。可能な設定については、後の項で説明します。

また、Mobile Link 同期サーバは、クライアントが送信したメッセージを復号化するため、独自の証明書用の秘密鍵を使用できる必要があります。秘密鍵は、Mobile Link 同期サーバが使用可能なファイルに保存されています。

図 1 に、Mobile Link 同期サーバが使用する証明書ファイルのサンプルを示します。この種類の証明書 (サーバ識別情報と呼びます) には、サーバの秘密鍵が含まれています。

```
-----BEGIN CERTIFICATE-----
MIIBqDCCAWSgAwIBAgIFMTIzNDUwCwYHKoZIzj0EAQUAMGsxDDAKBgNVBAYTA1VT
QTELMAkGA1UECBMCQ0ExEzARBgNVBAcTCkVtZXJ5dmlsbGUxFDASBgNVBAoUC1N5
YmFzZSBJbmMuMQ8wDQYDVQQLFAZTeWJhc2UxEjAQBgNVBAMUCVN5YmFzZSBDQTAe
Fw05OTExMTcxODA1MzZaFw0wOTExMTcxODA1MzZaMGcxDDAKBgNVBAYTA1VTQTEL
MAkGA1UECBMCQ0ExEzARBgNVBAcTCkVtZXJ5dmlsbGUxFDASBgNVBAoUC1N5YmFz
ZSBJbmMuMQwwCgYDVQQLFANNRUMxETAPBgNVBAMUCE1vYmlsaW5rMCswEAYHKoZI
zj0CAQYFK4EEAAEDFwACAx0L37T06bGehBNlRVJcma/Y0h5xoyYwJDAOBgNVHQ8B
Af8EBAMCAf4wEgYDVR0TAQH/BAgwBgEB/wIBCjALBgcqhkjOPQQBBQADMQAwLgIV
Ad+4IluT7/1URk7SfZTTiYqnR/rAAhUCCQRGc62100Mtt69TxusuwBvI2OY=
-----END CERTIFICATE-----
```

ルート証明書

```
-----BEGIN CERTIFICATE-----
MIIBrDCCAWigAwIBAgIFMTIzNDUwCwYHKoZIzj0EAQUAMGsxDDAKBgNVBAYTA1VT
QTELMAkGA1UECBMCQ0ExEzARBgNVBAcTCkVtZXJ5dmlsbGUxFDASBgNVBAoUC1N5
YmFzZSBJbmMuMQ8wDQYDVQQLFAZTeWJhc2UxEjAQBgNVBAMUCVN5YmFzZSBDQTAe
Fw05OTExMTcxODA0MjNaFw0wOTExMTcxODA0MjNaMGsxDDAKBgNVBAYTA1VTQTEL
MAkGA1UECBMCQ0ExEzARBgNVBAcTCkVtZXJ5dmlsbGUxFDASBgNVBAoUC1N5YmFz
ZSBJbmMuMQ8wDQYDVQQLFAZTeWJhc2UxEjAQBgNVBAMUCVN5YmFzZSBDQTArMBAG
ByqGSM49AgEGBSuBBAABAxcAAgFJVb7gQh0cy6XgxsRQUPaMCmIyk6MmMCQwDgYD
VR0PAQH/BAQDAgH+MBIGA1UdEwEB/wQIMAYBAf8CAQowCwYHKoZIzj0EAQUAAzEA
MC4CFQITRvY7k6c3jy37KyC4iDj6UNGWnQIVA/qAjA8SA2W7SyAfQ23oCY7n29Ss
-----END CERTIFICATE-----
```

サーバの証明書

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
ME4wGgYJKoZIhvcNAQUDMA0ECL+NqY7WeMr/AgEFBDAZTKkSUdCw2sUC45GKQaTR
xc1epiZwr9g5jm6wK8cCqOBfgZxs/Ne8eC2sn2klqlM=
-----END ENCRYPTED PRIVATE KEY-----
```

サーバの秘密鍵
(パスワードを使用
して暗号化)

図 1：サーバの証明書のサンプル

Mobile Link 同期サーバを実行しているマシンに他のユーザがアクセスする場合があるため、秘密鍵を含むファイルはパスワードで保護されます。このパスワードは、マシンへのアクセスを許可されたユーザが正規のユーザであることを前提としています。パスワードはわずか数文字で構成されているため、外部からの攻撃に対する有効な防御策としては機能しません。秘密鍵をさらに確実に保護するには、ファイアウォールなどの方法を使用して、外部から Mobile Link 同期サーバへのアクセスを拒否する必要があります。

サーバの証明書は、認証局が直接署名する代わりに、証明書チェーンの最初の証明書とすることができます。この場合は、クライアントがすべての証明書の所有者を信頼する必要があります。また、ルート証明書と呼ばれるチェーン内の最後の証明書の信頼されたコピーが必要です。この証明書ファイルは、図 1 に示す構造と類似した構造になっていますが、証明書のリストがさらに長くなることがあります。

セクション V：自己署名証明書

SQL Anywhere Studio には、証明書を処理するツールが付属しています。これらのツールは、ライセンスで許可されている場合は、配布内容に含まれています。その場合は、これらのセキュリティ・コンポーネントをインストールすることができます。

gencert というユーティリティを使用して、新しい証明書を生成することができます。証明書は、通常はマシンで読み取り可能なフォーマットで記述されています。readcert という別のユーティリティを使用すれば、証明書の内容をユーザが理解できるフォーマットで表示することができます。

gencert ユーティリティを使用して、さまざまな種類の証明書を作成することができます。自己署名 (ルート) 証明書は、他の署名が不要であるため、最も簡単に作成することができます。

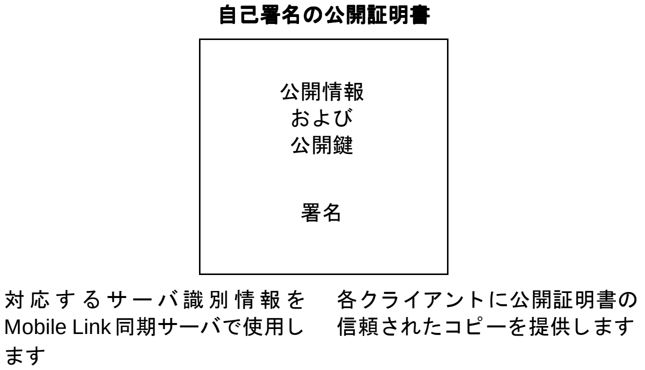


図 2：自己署名証明書

1 つのルート証明書だけを設定する場合の主な利点は、証明書を 1 つだけ作成すればよいという単純さです。この設定は、Mobile Link 同期サーバを 1 台だけ使用する設定では、ほとんどの場合十分です。複数の Mobile Link 同期サーバを使用するときは、多くの場合はエンタープライズ・レベルの証明書 (後述) が有用です。

最大の欠点は、他の証明書よりも自己署名証明書の方が偽造が簡単であるということです。この種類の攻撃としては、別の鍵の組み合わせを使用した偽造証明書の作成が挙げられます。他の種類の証明書は、複数のデジタル署名が含まれているため、セキュリティがより高くなっています。

自己署名証明書の作成

ルート証明書を作成するには、コマンド・プロンプトで、-r スイッチを指定して gencert ユーティリティを起動します。識別情報、証明書のパスワードおよび有効期限、新しい証明書ファイルの名前の入力が要求されます。

```
> gencert -r

Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink self-signed certificate
Serial Number: 2000.02.29.01
Certificate valid for how many years: 2
Enter password to protect private key: password
Enter file path to save certificate: self.crt
Enter file path to save private key: self.pri
Enter file path to save server identity: serv1.crt
```

各質問に対する回答は、文字列で入力します。ただし、期限切れまでの年数は整数で入力します。

入力した名前を使用して、3 つのファイルが作成されます。この例では、以下の 3 つのファイルが作成されます。

- `self.crt` このファイルには、識別情報、公開鍵、有効期限、署名を含む新しい証明書が保存されます。このファイルのコピーを接続先のユーザに提供します。

- `self.pri` このファイルには、証明書に含まれる公開鍵に対応した秘密鍵が含まれています。秘密鍵は、指定したパスワードで暗号化されています。これにより、自分のマシンにアクセスしようとする他のユーザに対してある程度のセキュリティを実現します。ただし、パスワードによる暗号化はそれほどセキュアではないため、機密性保持のためこのファイルへのアクセスを制限する必要があります。

- `serv1.crt` このファイルには、上記の 2 つのファイルの情報がまとめて含まれています。これは、Mobile Link 同期サーバで使用するファイルです。サーバは、クライアントに対して識別情報を提供するため、公開情報を送信します。クライアントが返信したメッセージを復号化するには、秘密鍵が必要です。このファイルへのアクセスは制限する必要があります。このファイルにも、パスワードだけで保護された秘密鍵が含まれています。

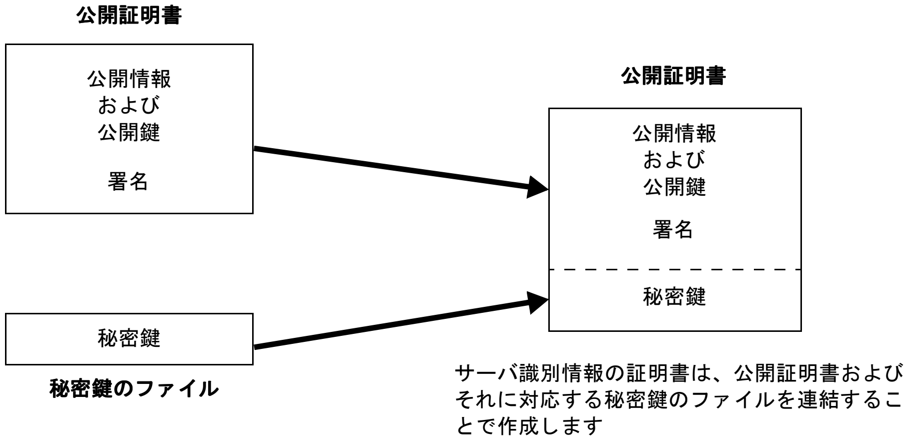


図 3：サーバの証明書の構成

サーバの証明書には、公開証明書と秘密鍵のファイルの情報が含まれています。サーバの証明書は、公開証明書および秘密鍵のファイルを連結して作成することができます。

自己署名証明書の使用

自己署名証明書をサーバ認証用に使用するには、以下の手順に従います。

1. 証明書のコピーをすべてのクライアントに提供します。クライアントが最初に Mobile Link 同期サーバに接続すると、サーバは公開証明書 self.crt のコピーをそのクライアントに送信します。クライアントは、サーバが送信した証明書と既存の証明書を比較することで、偽造された証明書を検出することができます。

2. 公開鍵 (配布済みの公開証明書のコピーに含まれています) で暗号化したメッセージを復号化できるサーバだけを信頼するように、各クライアントに指示します。Adaptive Server Anywhereクライアントの場合は、trusted_certificates というセキュリティ・パラメータを使用してこれを実行します。たとえば、以下のパラメータを SYNCHRONIZATION DEFINITION の ADDRESS 句に含めることで、Adaptive Server Anywhere クライアントに対して self.crt 証明書だけを信頼するように指示することができます。

   ```
   CREATE SYNCHRONIZATION DEFINITION test
   SITE 'user001'
   ADDRESS 'security=certicom_tls{trusted_certificates=self.crt}'
   (
     TABLE sales_order (id, cust_id, order_date, sales_rep ),
     TABLE customer (id, fname, lname, phone)
   )
   ```

   目的の証明書だけを信頼するように Ultra Light クライアントに指示するには、Ultra Light ジェネレータを実行する際に -r スイッチを使用して、信頼する証明書を指定します。コマンド全体を 1 行で入力します。

   ```
   > ulgen -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
   -r self.crt -j custapi

   Sybase Adaptive Server Anywhere UltraLite Code Generator Version
   7.0.0
   Running UltraLite analyzer
   Loading schema information
   Loading SQL statements
   Analyzing access plans
   Generating source code for SQL statements
   Generating source code for UltraLite schema
   Saving source code into database
   Writing source code to output file
   ```

3. Mobile Link 同期サーバを起動するときに、サーバの証明書ファイル名である serv1.crt および対応するパスワードを指定します。コマンド全体を 1 行で入力します。

   ```
   dbmlsrv7 -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
   -x tcpip{security=certicom_tls{certificate=serv1.crt;
          certificate_password=password}}
   ```

   クライアントには、秘密鍵やそれを解除するパスワードは不要であるため、これらは送信しないでください。クライアントに必要なのは公開証明書だけです。

   一方、Mobile Link 同期サーバでは、秘密鍵および証明書の公開部分にアクセスする必要があります。したがって、サーバはサーバの証明書ファイル (公開情報と秘密鍵の両方が含まれています) にアクセスする必要があります。

   Mobile Link 同期サーバでは、秘密鍵およびそれを保護するパスワードへのアクセスが必要です。このため、Mobile Link のコマンド・ラインおよびログ・ファイルを保護する必要があります。これには、ファイアウォールを使用するのが最適です。ファイアウォールを使用しない場合は、Mobile Link 同期サーバを実行するマシンへのアクセスを制限します。

セクション VI：認証局

自己署名証明書には、不正ユーザが別の公開鍵と秘密鍵の組を使用して証明書を偽造することができるという問題があります。偽造証明書を本物と間違えたユーザが、意図する相手の所有する公開鍵ではなく、別の公開鍵を使用して自分のメッセージを知らずに暗号化してしまう危険性があります。偽造証明書で暗号化したメッセージを読み取ることができるのは、その公開鍵に対応する秘密鍵を持つ不正ユーザだけです。

このような攻撃を防ぐには、ユーザと証明書の所有者の両方が第三者機関を信頼することに同意する必要があります。この第三者機関 (署名局または認証局と呼びます) は、自分の秘密鍵を使用して証明書にデジタル署名を追加します。署名後は、その第三者だけが証明書を変更することができます。認証局が証明書に署名する際に、証明書の所有者の秘密鍵機関は不要です。

認証局は、外部のユーザや組織である必要はありません。証明書を企業内でだけ使用する場合は、社員を認証局に任命するのが適している場合もあります。

信頼性の高いシステムを作成するには、認証局が証明書の所有者を慎重に確認してから、証明書に署名する必要があります。特に、証明書の識別情報のフィールドで証明書の所有者が正確に記述されていること、および証明書の所有者が対応する秘密鍵を所有していることを確認する必要があります。

この証明書を使用して所有者と通信を試みるユーザは、以下を確認する必要があります。

1. 証明書に署名する前に、証明書に含まれている識別情報が証明書の所有者と一致することを認証局が保証している。

2. 秘密鍵が証明書の所有者以外に公開されていない。

3. ユーザが特定の認証局の公開鍵の信頼できるコピーを入手している。

これらの条件を満たすには、ユーザが認証局を信頼しているだけでなく、その認証局から公開鍵を直接入手している必要があります。

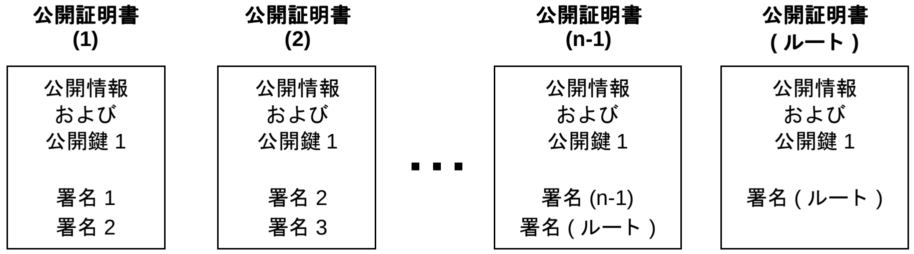
一般的に、公開鍵の有効なコピーを入手するには、認証局が所有する自己署名証明書のコピーを入手します。不正行為を防止するには、証明書を信頼できる手段で入手する必要があります。

また、各クライアントは、認証局の証明書を安全に保管する必要があります。不正ユーザがユーザのコンピュータへのアクセスに成功すると、認証局の証明書が偽造証明書に置き換えられる可能性があります。

セクション VII：証明書チェーン

レプリケーション・システムを配布する際には、多数の証明書が必要な場合があります。多数の証明書に署名する作業は、認証局にとって大きな負荷になることがあります。この負荷を軽減するため、認証局は署名の権限を委任することができます。委任するには、認証局が委任先の所有する証明書に署名します。委任先は、この証明書に含まれる秘密鍵を使用して、他の証明書に署名します。

証明書チェーンは、ある証明書が次の証明書に署名するという形式の、一連の証明書です。最後の証明書 (ルート証明書と呼びます) は、認証局が所有します。たとえば、サーバの証明書に委任先が署名します。委任先の証明書には、認証局が署名します。3 番目の証明書には、認証局の公開鍵が含まれています。この場合は、3 つの証明書のチェーンで構成されます。



対応するサーバ識別情報(1)をMobile Link同期サーバで使用します

各クライアントに公開のルート証明書の信頼されたコピーを提供します

図 4 : 証明書チェーン

実際には、委任先がさらに別の委任先を指定することができます。したがって、証明書チェーンは任意の長さにすることができます。ただし、最後の証明書は、常に自己署名のルート証明書であり、認証局が所有します。

チェーンを信頼するには、ユーザは以下を信頼する必要があります。

1. 証明書に署名する前に、証明書に含まれている識別情報が証明書の所有者と一致することを認証局およびすべての委任先が保証している。

2. 秘密鍵が証明書の所有者以外に公開されていない。

3. ユーザが特定の認証局の公開鍵の信頼できるコピーを入手している。

すべての条件は極めて重要です。証明書チェーンの強度は、最も弱いリンクの強度と同じです。

セクション VIII : エンタープライズのルート証明書

複数のサーバを使用する Mobile Link の配布では、共通のルート証明書で署名されたユニークな証明書を各サーバに割り当てることで、作業の効率を高めることができます。ルート証明書は、エンタープライズ内の認証局が所有します。

この方法には、以下の利点があります。

- 各 Mobile Link 同期サーバにユニークな証明書を割り当てることができるため、1 つのサイトに不正侵入されても他のサイトには影響を及ぼしません。

- エンタープライズのルート証明書の秘密鍵をMobile Link同期サーバに保存する必要がないため、セキュリティが向上します。

- クライアントは、公開ルート証明書のコピーだけを保存すればよく、各サーバの公開証明書のコピーを保存する必要はありません。これは、ルート証明書で署名された証明書はすべて信頼するようにクライアントを設定することができるためです。

グローバル署名証明書 (後述) を商用の認証局から入手することで、システムのセキュリティをある程度向上することができます。ただし、ここで説明する方法を使用すれば、多くのアプリケーションで実用上十分なセキュリティが実現します。

クライアントが一部の証明書のフィールドの値を確認するようにプログラムし (後述)、社内の特定の Mobile Link 同期サーバと同期するように設定することができます。

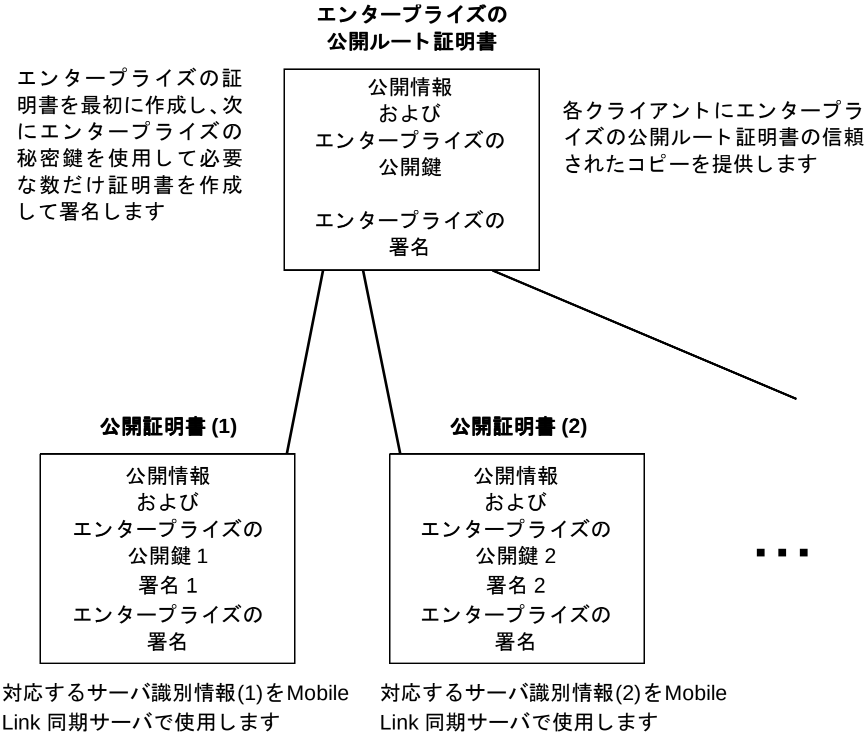


図 5：エンタープライズの証明書の使用

この設定では、サーバの自己署名証明書よりも柔軟な設定が可能です。たとえば、新しいサーバを追加し、新しい証明書を割り当てるとします。新しい証明書が同一のエンタープライズのルート証明書で署名されている場合は、既存のクライアントは自動的に新しい証明書を信頼します。Mobile Link 同期サーバに自己署名証明書を割り当てた場合は、すべてのクライアントで新しい公開証明書のコピーが必要になります。

証明書の作成

エンタープライズ・レベルのシステムを設定するには、最初に共通の自己署名証明書を生成します。共通のルート証明書を生成するには、-r スイッチを指定して gencert を起動します。

```
> gencert -c -r

Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink self-signed enterprise root
Serial Number: 2000.02.29.02
Certificate valid for how many years: 2
Enter password to protect private key: password2
Enter file path to save certificate: ent_root.crt
Enter file path to save private key: ent_root.pri
```

2 つのファイルが生成されます。

- **`ent_root.crt`** このファイルには、新しい証明書が含まれます。すべてのクライアントがこの証明書のコピーを必要とするため、この証明書は公開する必要があります。

- **`ent_root.pri`** このファイルには、証明書に含まれる公開鍵に対応した秘密鍵が含まれています。

これらのファイルは、別の新しい証明書の署名に使用することができます。署名付き証明書を生成するには、-s スイッチを指定して gencert を起動します。署名に使用する証明書ファイルの名前と、秘密鍵ファイルの名前およびパスワードを入力します。

```
> gencert -s
Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink server identity
Serial Number: 2000.02.29.03
Certificate valid for how many years: 1
Enter file path of signer’s certificate: ent_root.crt
Enter file path of signer’s private key: ent_root.pri
Enter password for signer’s private key: password2
Enter password to protect private key: password3
Enter file path to save server identity: serv1.crt
```

この場合は、gencert が生成するファイルは 1 つだけです。このファイルには、署名付き証明書および秘密鍵が含まれています。これは、Mobile Link 同期サーバで使用するファイルです。必要な回数だけ最後の手順を繰り返し、各 Mobile Link 同期サーバ用の署名付き証明書を作成します。

```
> gencert -s
Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
```

```
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink server identity
Serial Number: 2000.02.29.04
Certificate valid for how many years: 1
Enter file path of signer’s certificate: ent_root.crt
Enter file path of signer’s private key: ent_root.pri
Enter password for signer’s private key: password2
Enter password to protect private key: password4
Enter file path to save server identity: serv2.crt
```

この時点で作成したファイルは、以下のとおりです。

- ルート証明書 (ent_root.crt)
- ルートの秘密鍵 (ent_root.pri)
- ルートの結合証明書 (ent_serv.crt)
- 最初の Mobile Link 同期サーバ用の結合証明書 (serv1.crt)
- 2 番目の Mobile Link 同期サーバ用の結合証明書 (serv2.crt)

Mobile Link 同期サーバは結合ルート証明書を直接使用するため、この証明書は必要ありません。その代わり、各 Mobile Link 同期サーバ用に個別の証明書を作成しました。

署名付き証明書の使用

署名付き証明書をサーバ認証用に使用するには、以下の手順に従います。

1. 公開のルート証明書のコピーをすべてのクライアントに配布します。クライアントが最初に Mobile Link 同期サーバに接続すると、サーバは独自の公開証明書のコピーをクライアントに送信します。この証明書は、ルート証明書で署名されています。クライアントは、ルートの署名がクライアント側のルート証明書のコピーの公開鍵とを比較して、偽造証明書を検出することができます。

2. 証明書にルート証明書の署名があるサーバだけを信頼するように、各クライアントに指示します。Adaptive Server Anywhere クライアントの場合は、trusted_certificates というセキュリティ・パラメータを使用します。たとえば、このパラメータを以下のように SYNCHRONIZATION DEFINITION の ADDRESS 句に含めることで、Adaptive Server Anywhere クライアントに対して ent_cert.crt 証明書だけを信頼するように指示することができます。

   ```
   CREATE SYNCHRONIZATION DEFINITION test
   SITE ’user001’
   ADDRESS
   ’security=certicom_tls{trusted_certificates=ent_cert.crt}’
   ```

目的の証明書だけを信頼するように Ultra Light クライアントに指示するには、以下のように、Ultra Light ジェネレータを実行する際に -r スイッチを使用して、信頼する証明書を指定します。コマンド全体を 1 行で入力します。

```
> ulgen -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
-r ent_cert.crt -j custapi
Sybase Adaptive Server Anywhere UltraLite Code Generator Version
7.0.0
Running UltraLite analyzer
Loading schema information
Loading SQL statements
Analyzing access plans
Generating source code for SQL statements
Generating source code for UltraLite schema
Saving source code into database
Writing source code to output file
```

3. 各 Mobile Link 同期サーバを起動するときに、サーバの証明書ファイル名および対応するパスワードを指定します。コマンド全体を 1 行で入力します。

```
dbmlsrv7 -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
-x tcpip{port=3333;security=certicom_tls{certificate=serv1.crt;
       certificate_password=password3}}
dbmlsrv7 -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
-x tcpip{port=4444;security=certicom_tls{certificate=serv2.crt;
       certificate_password=password4}}
```

セクション IX：グローバル署名証明書

複数のサーバを使用する Mobile Link の配布では、共通のルート証明書で署名されたユニークな証明書を各サーバに割り当てることで、作業の効率を高めることができます。商用の認証局が署名した証明書を使用することで、配布がさらに簡単になります。このような証明書を、グローバル証明書またはグローバル署名証明書と呼びます。商用の認証局は、高品質の証明書を作成し、これらの証明書を使用して他の証明書の署名を行う組織です。

グローバル証明書には、以下の利点があります。

- セキュリティ上、通信を行う両者がルート証明書を信頼する必要があります。認証局は、署名対象のすべての証明書で識別情報の正確性を保証する必要があるため、企業間通信の場合は、外部の共通の公認された認証局を使用して、システムのセキュリティを向上します。

- 高品質の疑似乱数データを使用して鍵を作成することで、セキュリティが向上します。gencert ユーティリティで使用されるデータは暗号化用のデータですが、管理された環境で他のさらに優れた方法を使用することもできます。

- ルート証明書の秘密鍵は、保護しておく必要があります。企業によっては、この重要な情報を保存する適切な場所がない場合がありますが、認証局は専用の設備を設計および管理しています。

グローバル署名証明書を使用する場合は、各クライアントが証明書のフィールドの値を確認し、同一の認証局によって他のクライアント用に署名された証明書を信頼しないようにする必要があります。この処理については、次の項で説明します。

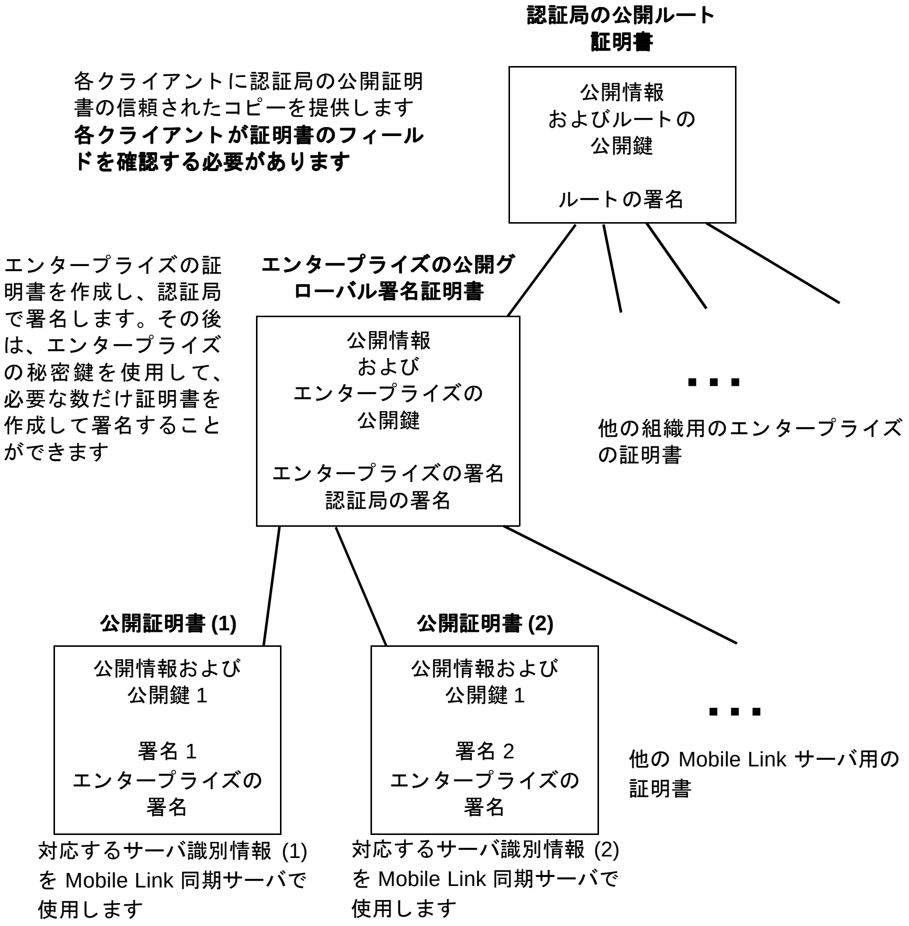


図 6：**エンタープライズのグローバル署名証明書の使用**

Mobile Link のトランスポート・レイヤのセキュリティは、Certicom SSL/TLS Plus ライブラリを基盤としています。このライブラリでは、楕円曲線証明書が必要です。グローバル証明書は、Certicom などの、適切なフォーマットで証明書を提供する認証局から入手することができます。

Certicom からのグローバル証明書の入手

Certicom は、適切なフォーマットで証明書を提供する認証局です。グローバル証明書およびエンタープライズ・レベルの署名付き証明書を Certicom から入手するには、以下の手順に従います。

1. Mobile Link のトランスポート・レイヤのセキュリティ・コンポーネントに付属の reqtool ユーティリティを使用して、サーバ証明書およびグローバル証明書を要求します。

2. 公開証明書の内容をクリップボードにコピーします。

3. Certicom MobileTrust の Web サイト (http://www.certicom.com/mobiletrust/ecommerceserver/) で、ライセンス・ポリシーを確認し、支払方法を選択します。

4. 公開証明書の内容を MobileTrust の Web サイト上のフォームにペーストします。証明書の要求の公開部分だけを送信します。*秘密鍵は送信しないでください*。

5. Certicom MobileTrust Registration Agent が要求を処理します。処理が終了すると、通常は電話で連絡があり、パスワードを通知されます。このパスワードを使用して、MobileTrust の Web サイトからグローバル証明書を入手することができます。

この手順の詳細については、Mobilink の bin または win32 ディレクトリにある reqtool.pdf を参照してください。

reqtool ユーティリティの実行

SQL Anywhere Studio に付属する reqtool は、Certicom に送信する、サーバ証明書およびグローバル証明書の要求用ドキュメントを作成します。このユーティリティの使用方法は、以下のとおりです。Mobile Link と互換性のある鍵の種類は、*楕円曲線暗号化* (ECC) だけです。

```
> reqtool

-- Certicom Corp. Certificate Request Tool 3.0d1 --

Choose certificate request type:
  E - Personal email certificate request.
  S - Server certificate request.
  Q - Quit.
Please enter your request [Q] : S

Choose key type:
  R - RSA key pair.
  D - DSA key pair.
  E - ECC key pair.
  Q - Quit.
Please enter your request [Q] : E
Using curve ec163a02. Generating key pair (please wait)...
Country: CA
State: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink
Enter password to protect private key : password5
Enter file path to save request : global.req
Enter file path to save private key : global.pri
```

global.req というファイルには、公開証明書および要求情報が含まれています。このファイルの内容を、MobileTrust の Web サイト上のフォームにペーストします。

global.pri というファイルには、エンタープライズの証明書の秘密鍵が含まれています。このファイルは、指定したパスワードで保護されていますが、パスワードによる保護は強力ではないため、このファイルを安全な場所に保存する必要があります。

Certicom MobileTrust Registration Agent により、要求が処理されます。処理が終了すると、通常は電話で連絡があり、パスワードを通知されます。このパスワードを使用して、MobileTrust の Web サイトからグローバル証明書を入手することができます。すぐに証明書をダウンロードします。証明書は、バイナリ・フォーマットとテキスト・フォーマットの 2 種類のフォーマットで受信することができます。いずれのファイルにも、同一の情報が含まれています。この場合は、テキスト・フォーマットの証明書を、global.crt という名前のファイルに保存します。

サーバの証明書としてグローバル証明書を使用する

グローバル証明書を Mobile Link 同期サーバの証明書として直接使用することができます。この場合は、公開証明書と秘密鍵を連結して、サーバの証明書を作成します。Windows のコマンド・プロンプトで、以下のコマンドを入力します。

```
copy global.crt+global.pri global2.crt
```

これで、新しい証明書および秘密鍵のパスワードを指定して、Mobile Link 同期サーバを起動することができます。コマンド全体を 1 行で入力します。

```
dbmlsrv7
-c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql" -x
tcpip{security=certicom_tls{certificate=global2.crt;
certificate_password=password5}}
```

また、Mobile Link 同期サーバに接続を試みるクライアントが証明書を信頼する必要があります。これには、チェーンのルート証明書を信頼するようにクライアントに指示する必要があります。この場合のチェーンのルート証明書は、認証局が所有する証明書です。

デフォルトでは、Mobile Link クライアントは、Certicom のルート証明書か、Mobile Link に付属のサンプル証明書の署名に使用した Sybase のルート証明書のいずれかによって署名された証明書を信頼します。したがって、Certicom がグローバル証明書に署名する場合は、Mobile Link クライアントは自動的にその証明書を有効なものと判断します。

ただし、セキュリティを高めるため、クライアントが認証局のルート証明書だけを有効として認める必要があります。

この証明書だけを SQL の CREATE SYNCHRONIZATION DEFINITION 文の ADDRESS 句で指定すると、Certicom のルート証明書だけを有効として認めるように Adaptive Server Anywhere Mobile Link クライアントに指示することができます。

```
CREATE SYNCHRONIZATION DEFINITION test
SITE 'user001'
ADDRESS 'security=certicom_tls{trusted_certificates=certicom.crt}'
```

Certicom のルート証明書だけを信頼するように Ultra Light クライアントに指示するには、Ultra Light ジェネレータを実行する際に -r スイッチを使用して、信頼する証明書を指定します。コマンド全体を 1 行で入力します。

```
> ulgen -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql"
-r certicom.crt -j custapi

Sybase Adaptive Server Anywhere UltraLite Code Generator Version
7.0.0
Running UltraLite analyzer
Loading schema information
Loading SQL statements
Analyzing access plans
Generating source code for SQL statements
Generating source code for UltraLite schema
Saving source code into database
Writing source code to output file
```

手間を省くため、certicom.crt というファイルが Mobile Link に付属しています。ただし、必要であれば Certicom から直接証明書のコピーを入手することもできます。

セクション X：証明書のフィールドの確認

グローバル証明書は、場合によっては重大な問題を引き起こす危険性があります。Mobile Link のクライアントを上記のように設定した場合には、認証局が署名したすべての証明書を信頼するため、同一の認証局が別の企業に対して発行した証明書も信頼する可能性があります。証明書を区別する方法がなければ、クライアントは競合他社の Mobile Link 同期サーバを自社のサーバと判断し、機密情報を誤送信する危険性があります。

他の場合にも、同様の注意が必要なことがあります。企業がエンタープライズの証明書を使用する場合でも、Mobile Link クライアントの接続先の部門を確認することが重要です。

この問題は、証明書の識別情報のフィールドの値を確認するようにクライアントに要求することで解決できます。証明書で確認可能なフィールドは 3 つあります。これらのフィールドのいずれかまたはすべてを確認することができます。

1. 組織

2. 組織単位

3. 共通名

これらのフィールドを確認するには、有効な値を指定します。たとえば、次のコードは、3 つのフィールドをすべて確認し、指定した値だけを有効と認めるように Adaptive Server Anywhere クライアントに指示します。SQL 文全体を 1 行で入力します。

```
CREATE SYNCHRONIZATION DEFINITION test
SITE 'fuser'
ADDRESS 'port=3333;security=certicom_tls{
       trusted_certificates=certicom.crt;
```

```
        certificate_company=Sybase, Inc.;
        certificate_unit=MEC;certificate_name=MobiLink}'
```

Ultra Light クライアントの場合も、同様の方法でフィールドを確認することができます。実際の構文は、アプリケーションの構築に使用したインタフェースによって異なります。C 言語で記述した次のコードは、Ultra Light アプリケーションを C または C++ で作成した場合と同様のタスクを実行します。

```
ul_synch_info info;

. . .

info.security_parms =
      UL_TEXT( "certificate_company=Sybase, Inc." )
      UL_TEXT( ";" )
      UL_TEXT( "certificate_unit=MEC" )
      UL_TEXT( ";" )
      UL_TEXT( "certificate_name=MobiLink" );

. . .

ULSynchronize( &info );
```

この例は、3 つのフィールドをすべて確認します。フィールドを 1 つまたは 2 つだけ確認することもできます。

証明書チェーンのフィールドの確認

最初の証明書がチェーンの一部である場合は、指定したフィールドのすべての値がその証明書でチェックされます。指定した場合は、ルート証明書を除く他のすべての証明書で、企業名もチェックされます。これは、ルート証明書を認証局が所有する場合にも該当します。この場合は、ルート証明書をユーザの企業または組織ではなく認証局が所有するため、フィールド値が異なります。

エンタープライズ証明書としてのグローバル署名証明書の使用

グローバル証明書をサーバの証明書として使用する代わりに、エンタープライズの証明書などの他の証明書の署名に使用することもできます。この場合は、グローバル証明書とエンタープライズの証明書の両方の利点を活用することができます。最も重要な利点は、グローバル証明書の秘密鍵を、Mobile Link 同期サーバを実行するコンピュータに保存する必要がないことです。

注

認証局は、独自の裁量で、他の証明書の署名に使用可能な証明書を販売していない場合があります。しかるべき注意を払わずに証明書に署名すると、セキュリティが低下し、場合によっては認証局の信用低下につながります。たとえば、Certicom の証明書はこのような方法で使用することはできません。詳細については、担当の認証局にお問い合わせください。

グローバル署名証明書をエンタープライズの署名として使用するには、各 Mobile Link 同期サーバ用にユニークな証明書を作成します。この場合は、自分のグローバル証明書で各サーバの証明書に署名します。次の例で、サーバの証明書を生成し、グローバル証明書で署名する方法を説明します。

```
> gencert -s

Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink
Serial Number: 2000.02.29.06
Certificate valid for how many years: 1
Enter file path of signer's certificate: global.crt
Enter file path of signer's private key: global.pri
Enter password for signer's private key: password5
Enter password to protect private key: password6
Enter file path to save server identity: serv6.crt

> gencert -s

Sybase Elliptic Curve Certificate Generation Tool
Generating key pair using curve ec163a02 (please wait)...
Country: CA
State/Province: Ontario
Locality: Waterloo
Organization: Sybase, Inc.
Organizational Unit: MEC
Common Name: MobiLink
Serial Number: 2000.02.29.07
Certificate valid for how many years: 1
Enter file path of signer's certificate: global.crt
Enter file path of signer's private key: global.pri
Enter password for signer's private key: password5
Enter password to protect private key: password7
Enter file path to save server identity: serv7.crt
```

上記のコマンドは、Mobile Link 同期サーバで使用するためのサーバの証明書を 2 つ生成します。

- Mobile Link 同期サーバ 1 用の証明書は serv6.crt です。
- Mobile Link 同期サーバ 2 用の証明書は serv7.crt です。

両方の証明書は、global.crt で署名されます。global.crt は、Certicom のルート証明書で署名されます。

これらの 2 つの Mobile Link 同期サーバは、以下のコマンドを使用して起動します。コマンドは、1 行に 1 つずつ入力します。

```
dbmlsrv7 -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql" -x
tcpip{port=3333;security=certicom_tls{certificate=serv6.crt;
certificate_password=password6}}

dbmlsrv7 -c "dsn=UltraLite 7.0 Sample;uid=dba;pwd=sql" -x
tcpip{port=4444;security=certicom_tls{certificate=serv7.crt;
certificate_password=password7}}
```

また、各クライアントが Certicom のルート証明書を信頼するように設定する必要があります。Certicom 以外の認証局を使用する場合は、クライアントがその認証局の証明書だけを信頼するように設定します。

Mobile Link クライアントが Certicom のルート証明書だけを信頼するようにする手順は、前述したとおりです。

セクション XI：Palm クライアントでの証明書の使用

他の Mobile Link クライアントと同様に、Paml Computing プラットフォームで実行する Ultra Light アプリケーションでもデジタル証明書を利用することができます。ただし、同期は 2 つの方法のいずれかでだけ実行することができます。Palm アプリケーションの同期方法によって、接続で保護される部分、およびトランスポート・レイヤのセキュリティに関するクライアント設定情報が保存される場所が異なります。

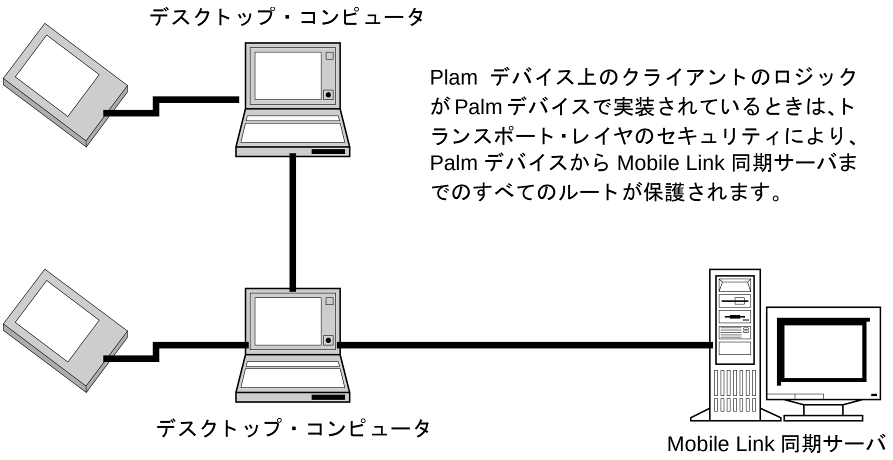
Palm Computing プラットフォーム上の Ultra Light アプリケーションは、2 つの方法のいずれかで同期を実行します。

1. Mobile Link 同期サーバに直接接続する

2. HotSync または ScoutSync を使用してデスクトップ・コンピュータに接続し、Mobile Link コンジットを使用して Mobile Link 同期サーバに接続する

直接接続の使用

最初の方法では、すべての Mobile Link クライアントのロジック (トランスポート・レイヤのセキュリティを含む) は Palm デバイスで実装されます。このような Palm アプリケーションが同期を実行する場合は、すべてのメッセージが Palm デバイス上で暗号化または復号化されます。これらのメッセージは、ネットワークに接続されたコンピュータを経由することがありますが、ルート全体で Mobile Link のトランスポート・レイヤのセキュリティによりメッセージが保護されています。



Plam デバイス上のクライアントのロジックがPalm デバイスで実装されているときは､トランスポート･レイヤのセキュリティにより､Palm デバイスから Mobile Link 同期サーバまでのすべてのルートが保護されます。

図 7：直接接続による同期

すべての Mobile Link クライアントのロジックは Palm デバイス上で実装されているため、すべてのクライアント設定も Palm デバイス上に保存されます。Ultra Light クライアントの場合は、Ultra Light のジェネレータで -r スイッチを使用して、信頼されたルート証明書を指定します。

HotSync または ScoutSync の使用

2 番目の方法では､Palm Computing プラットフォームで HotSync または ScoutSync を利用して、他のコンピュータと情報を交換します。これらのアプリケーションは、デスクトップ・コンピュータとの間での個人データの同期を管理するために使用します｡Palm デバイスは、設定に従って、直接接続されたコンピュータとデータを交換するか、HotSync または ScoutSync のプロキシおよびサーバのコンジット・マネージャを使用して、別の場所にある他のコンピュータとデータを交換します。

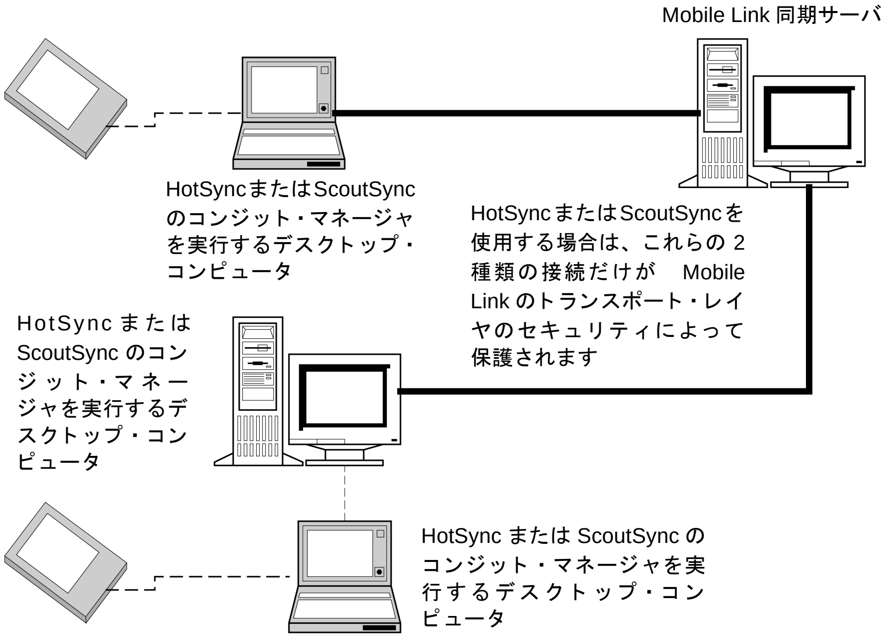


図 8：HotSync または ScoutSync を使用した同期の実行

HotSync または ScoutSync を基盤とする同期は、Palm デバイスまたはクレードルから実行することができます。接続先では、HotSync または ScoutSync のコンジット・マネージャが Mobile Link のコンジット DLL を呼び出します。これらの DLL には、Mobile Link クライアントのロジックが含まれています。これらのロジックは、HotSync または ScoutSync 固有の API を使用して Palm デバイスにアクセスします。HotSync または ScoutSync では、DLL が Palm デバイス上の Palm データベースのレコードの読み書きを実行することができます。

HotSync および ScoutSync では、シリアル接続、電話回線、LAN、ワイヤレス・ネットワークで同期を実行することができます。ただし、この通信は Mobile Link システムの一部ではないため、Mobile Link のトランスポート・レイヤのセキュリティでは保護されません。したがって、通常の電話回線、公衆ネットワーク、ワイヤレス・モデムで HotSync や ScoutSync を使用すると、通信チャネルのその部分が攻撃に対して脆弱になります。

これに関連するセキュリティ問題の多くは、仮想プライベート・ネットワークなどのソフトウェアや、セキュアなポイント・ツー・ポイントのルータなどのハードウェアを使用して改善することができます。ネットワーク管理者またはコンジットの製造元から、追加情報を入手できることがあります。

Palm クレードルを使用して、Mobile Link コンジットの DLL を実行しているコンピュータに Palm デバイスを直接接続するのが、多くの場合に単純で有効な解決方法です。この方法では、HotSync または ScoutSync を使用して転送されるデータへのアクセスが制限されるため、データ保護が実現します。

HotSync または ScoutSync を使用する場合の Mobile Link クライアントのパラメータ設定

HotSync または ScoutSync を使用する場合は、Mobile Link クライアントのロジックは Palm デバイスではなく、Mobile Link コンジットを実行するコンピュータに実装されます。したがって、証明書のフィールドのチェックや信頼されたルートを制御する Mobile Link クライアントのパラメータは、Mobile Link コンジットを実行するマシンで設定する必要があります。

これらのパラメータを設定する方法は 2 通りあります。

1. ul_synch_info データ構造体のパラメータを設定し、この構造体への参照を Ultra Light アプリケーションでの PalmExit 呼び出しへのパラメータとして引き渡します。この値は、自動的に HotSync または ScoutSync を使用して転送され、接続先の Mobile Link コンジットで使用されます。

2. Mobile Link コンジットを実行するマシンのレジストリにエントリを追加します。エントリの追加は、HotSync や ScoutSync のコンジット・マネージャが提供する設定機能を使用して行うことができます。これらの値を設定する方法およびレジストリでの値の位置は、コンジット・マネージャによって異なります。

セクション XII：セキュリティのチェックリスト

効果的なセキュリティを実現するには、開発および展開のプロセスでセキュリティが重要になります。Mobile Link のトランスポート・レイヤのセキュリティなどのセキュア・メカニズムを使用しても、システムへの他のアクセス・ポイントを見過ごしては意味がありません。以下に示すチェックリストは、包括的なものではありませんが、一般的な多くの脆弱部分を改善する際の参考として説明します。

1. Mobile Link 同期サーバを実行するコンピュータへのアクセスを制限します。サーバは、サーバの証明書ファイル (公開情報と秘密鍵の両方が含まれています) にアクセスする必要があります。証明書のパスワードによってある程度の保護が実現されますが、サーバのコンピュータを使用するユーザには、コマンド・ラインで指定すればファイルが表示されてしまいます。

2. 統合データベース・サーバへのアクセスを制限します。このサーバは、Mobile Link 同期サーバと同一のコンピュータで実行されている場合と、そうでない場合があります。このデータベースには、データのマスタ・コピーの他に、同期プロセスを制御するスクリプトも含まれています。すべてのアカウント、特に機密データや設定を変更できるアカウントのパスワードを推測されないようにしてください。同様に、信頼できないユーザには、システムのセキュリティ設定を変更する権限を与えないでください。これを実現するには、コンピュータへのアクセスを制限するのが最も簡単です。

3. Mobile Link 同期サーバおよび統合データベース・サーバを別のコンピュータで実行する場合は、両者を接続するネットワークを保護します。現在は、2 つのネットワーク・ロケーション間でのデータの認証および暗号化を行う専用のネットワーク・ハードウェアを使用することができます。また、一方のマシンのポートからもう一方のマシンのポートへの TCP/IP 通信を暗号化できるソフトウェア・ソリューションを使用することもでき

ます。仮想プライベート・ネットワーク (VPN) または最先端の IP セキュリティ・プロトコルを使用して、コンピュータ間の接続を保護することもできます。

4. すべてのクライアントが、1 つのルート証明書 (サーバの証明書の署名に使用した証明書) だけを信頼するようにします。デフォルトでは、Mobile Link クライアントは 2 つの異なるルート証明書、つまり Sybase と Certicom のルート証明書を信頼するように設定されています。このデフォルト設定は、開発時には便利ですが、配布するシステムでは必ず変更してください。Adaptive Server Anywhere Mobile Link クライアントの場合は、trusted_certificates というセキュリティ・ストリーム・パラメータを使用して、信頼された証明書を指定します。Ultra Light Mobile Link クライアントの場合は、ulgen ユーティリティで -r スイッチを使用します。

5. すべてのクライアントが証明書のフィールドを確認するようにします。認証局は、同一のルート証明書を使用して他のエンティティの証明書に署名する場合があります。アプリケーションがサーバの証明書のフィールドを使用して、自分のエンティティまたは企業に所属する証明書を確認しない場合、クライアントはすべての証明書を有効と見なします。Mobile Link クライアントは、certificate_company、certificate_unit、certificate_name というストリーム・パラメータを使用して、証明書の所有者を確認することができます。

6. Palm アプリケーションで HotSync または ScoutSync を使用する場合は、HostSync または ScoutSync のデータ転送に使用するすべての接続およびコンピュータを保護します。Mobile Link のトランスポート・レイヤのセキュリティは、Mobile Link クライアントと Mobile Link サーバ間の通信だけを保護するように設計されています。HotSync または ScoutSync を使用する場合は、クライアントになるのは Mobile Link コンジットを実行するコンピュータです。したがって、トランスポート・レイヤのセキュリティでは、このコンピュータと Mobile Link サーバ間の通信だけが保護されます。

7. Mobile Link クライアントへのアクセスを制限します。各クライアントは、公開ルート証明書の信頼されたコピーを保存する必要があります。このコピーが変更または置換されると、クライアントが別の Mobile Link サーバに接続するように偽装される可能性があります。クライアント・デバイスそのものでは情報が暗号化されて保存されていても、このような攻撃により、機密情報が不正ユーザに漏洩する危険性があります。

結論

サーバが 1 台だけの場合は、自己署名証明書を作成するのが最も簡単な設定です。この場合の唯一の欠点は、証明書の秘密鍵をより強固な保護の同期サーバに保存する必要がある点です。

エンタープライズのルート証明書は、複数の Mobile Link 同期サーバを使用する企業には特に有効です。Mobile Link クライアントはこのルート証明書のコピーを保存するだけで、このルート証明書で署名された証明書を発行するすべての Mobile Link 同期サーバを認識することができます。

最高のセキュリティが要求される企業では、商用の認証局を利用するのが有効な場合があります。商用の認証局は、2 つの点で有用です。第一に、商用の認証局が使用するルート証明書は、理想的な高品質を提供し、攻撃対象となる可能性を抑えます。第二に、商用の認証局は、お互いになじみのない企業がセキュアな通信を実行する場合に、信頼された第三者として機能することができます。

証明書のフィールドを確認するための機能を使用することができます (場合によっては必須)。これは、グローバル署名証明書を使用する場合に特に該当します。この場合は、認証局が他の顧客用に署名した証明書をクライアントが信頼する危険性はありません。

いずれの場合も、Mobile Link のコマンド・ラインおよびログ・ファイルを保護する必要があります。これには、ファイアウォールを使用するのが最適です。ファイアウォールを使用しない場合は、Mobile Link 同期サーバを実行するマシンへのアクセスを制限します。

Mobile Link のトランスポート・レイヤのセキュリティは、設定に重要なセキュリティを実現するための柔軟なメカニズムです。基本システムは、情報の機密性を保護することができます。さらに、証明書を使用することで、Mobile Link クライアントは信頼された Mobile Link 同期サーバと通信することができます。

※本書は、米国 iAnywhere Solutions 社が作成およびテストしたものを日本語に翻訳したものです。

法的注意

Adaptive Server、iAnywhere、iAnywhere Solutions、SQL Anywhere、SQL Anywhere、Sybaseは、米国法人iAnywhere Solutions, Inc.または米国法人Sybase,Inc.とその系列会社の米国または日本における登録商標または商標です。その他の商標はすべて各社に帰属します。

Mobile Linkの技術には、Certicom,Inc.より供給を受けたコンポーネントが含まれています。これらのコンポーネントは特許によって保護されています。

本書に記載された情報、助言、推奨、ソフトウェア、文書、データ、サービス、ロゴ、商標、図版、テキスト、写真、およびその他の資料(これらすべてを"資料"と総称する)は、iAnywhere Solutions, Inc.とその供給元に帰属し、著作権や商標の法律および国際条約によって保護されています。また、これらの資料はいずれも、iAnywhere Solutions, Inc./Sybとその供給元の知的所有権の対象となるものであり、iAnywhere Solutions, Inc./Sybase,Inc.とその供給元がこれらの権利のすべてを保有するものとします。

資料のいかなる部分も、iAnywhere Solutionsの知的所有権のライセンスを付与したり、既存のライセンス契約に修正を加えることを認めるものではないものとします。

資料は無保証で提供されるものであり、いかなる保証も行われません。iAnywhere Solutionsは、資料に関するすべての陳述と保証を明示的に拒否します。これには、商業性、特定の目的への整合性、非侵害性の黙示的な保証を無制限に含みます。

iAnywhere Solutionsは、資料自体の、または資料が依拠していると思われる内容、結果、正確性、適時性、完全性に関して、いかなる理由であろうと保証や陳述を行いません。iAnywhere Solutionsは、資料が途切れていないこと、誤りがないこと、いかなる欠陥も修正されていることに関して保証や陳述を行いません。ここでは、「iAnywhere Solutions」とは、iAnywhere Solutions,Inc.とその部門、子会社、継承者、および親会社と、その従業員、パートナー、社長、代理人、および代表者と、さらに資料を提供した第三者の情報元や提供者を表します。

＊　本書は、米国iAnywhere Solutions, Inc.が作成・テストしたものを日本語に翻訳したものです。

アイエニウェア・ソリューションズ株式会社
http://www.ianywhere.jp