Mobile Link のエンドツーエンド暗号化

Joshua Savill
September 8th, 2008

This whitepaper was written in the context of SQL Anywhere 11.

CONTENTS

FIGURES

はじめに

SQL Anywhere 11 には、Mobile Link または Ultra Light クライアントと Mobile Link サーバ間をプロトコル・レベルで暗号化できる新しい Mobile Link 機能が搭載されています。これは、RSA と ECC の両方の暗号化タイプをサポートするエンドツーエンド暗号化機能です。

Mobile Link の同期セキュリティ

SQL Anywhere 11 よりも前のバージョンで Mobile Link 同期データ・ストリームを暗号化する場合には、TLS (Transport Layer Security ：トランスポート層セキュリティ) を使用するしかありませんでした。しかし、TLS には、同期データ・ストリームを復号化してから特定のデータ同期環境で再暗号化するために仲介役が必要になるというデメリットがあります。Web サーバ経由の HTTPS 同期で必要になることが多いこのような仲介役を介してデータの復号化と再暗号化を行うと、WAP ギャップが生じます。ここでは、データが暗号化されないまま送信され、危険にさらされる可能性があります。図 1 は、WAP ギャップを介して送信される Mobile Link 同期データ・ストリームを示したものです。

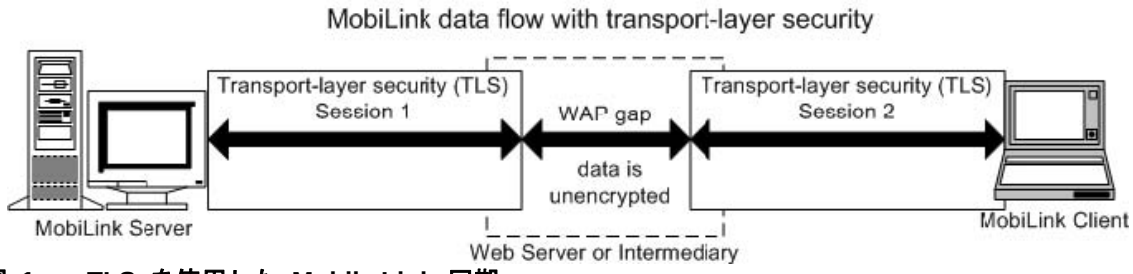

図 1 - TLS を使用した Mobile Link 同期

次に、図 2 をご覧ください。Mobile Link または Ultra Light クライアントと Mobile Link サーバ間で送信される Mobile Link 同期データ・ストリームがエンドツーエンド暗号化によって保護されています。この図からわかるように、データが暗号化されたままの状態で仲介役の中を通過するため、データ・ストリームを復号化してから再暗号化する必要がありません。

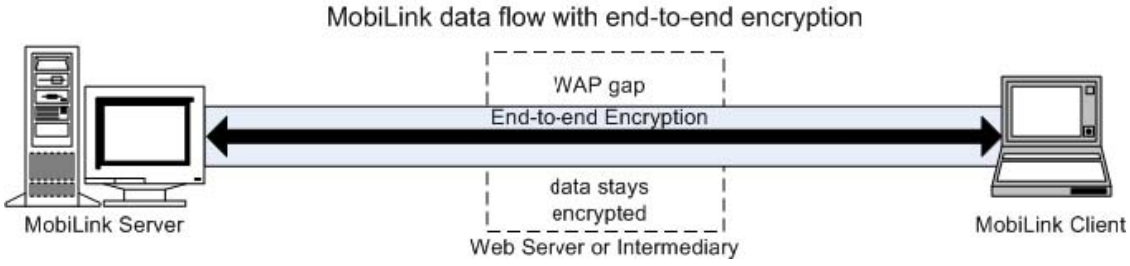

図 2 - WAP ギャップの中を通過するエンドツーエンド暗号化を使用した Mobile Link 同期

このエンドツーエンド暗号化と TLS を組み合わせて使用すれば、セキュリティの向上を図ることもできます。図 3 は、Mobile Link 同期データ・ストリームにエンドツーエンド暗号化だけでなく TLS も適用したネットワーク構成を示したものです。

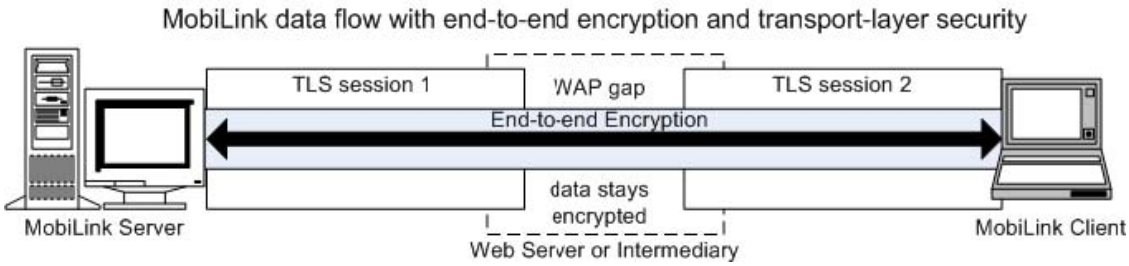

図 3 - エンドツーエンド暗号化と TLS を併用した Mobile Link 同期

SQL Anywhere 11 の Mobile Link 機能の 1 つであるエンドツーエンド暗号化機能は、RSA と ECC の両方の暗号化タイプをサポートしています。TLS と HTTPS の各プロトコルでこのエンドツーエンド暗号化を行う場合には、FIPS オプションを有効にすることもできます。たとえば、このオプションを暗号化タイプとして指定すると、Mobile Link サーバおよびクライアントが FIPS 1402 承認の RSA 暗号化を使用することになります。ただし、ECC 暗号化タイプを使用している場合は、このオプションを指定できません。

エンドツーエンド暗号化を有効にする方法

Mobile Link サーバ

Mobile Link サーバのエンドツーエンド暗号化は、新しいオプションと –x コマンド・ライン・スイッチを使用して有効にします。その際には、以下の 3 つのオプションを指定します。

e2ee_type=type

このオプションでは、セッション・キーの交換に使用するキーのタイプを指定できます。使用可能な暗号化タイプは RSA と ECC です。ただし、暗号化タイプは、プライベート・キー・ファイルに指定したキー・タイプと一致していなければなりません。e2ee_type のデフォルト値は RSA です。

e2ee_private_key=file

このオプションでは、RSA または ECC プライベート・キーが保存されている PEM エンコード・ファイルのロケーションを指定できます。このエンコード・ファイルは、Mobile Link データ・ストリームを暗号化する際に必要になります。

e2ee_private_key_password=password

このオプションでは、PEM エンコード・ファイルのパスワードを指定できます。このパスワードは、PEM エンコード・ファイルにアクセスしてから Mobile Link データ・ストリームを暗号化する際に必要になります。

Mobile Link および Ultra Light クライアント

Mobile Link および Ultra Light クライアントのエンドツーエンド暗号化は、同期開始時に新しい Mobile Link クライアント接続オプションを使用して有効にします。その際には、以下の 2 つのオプションを指定します。

e2ee_type=type

このオプションでは、セッション・キーの交換に使用するキーのタイプを指定できます。使用可能な暗号化タイプは RSA と ECC です。ただし、暗号化タイプは、プライベート・キー・ファイルに指定したキー・タイプのほか、Mobile Link サーバ上で指定したキー・タイプと一致していなければなりません。e2ee_type のデフォルト値は RSA です。

e2ee_public_key=file

このオプションでは、RSA または ECC パブリック・キーが保存されている PEM エンコード・ファイルのロケーションを指定できます。このエンコード・ファイルは、Mobile Link クライアント・データ・ストリームを暗号化する際に必要になります。

Note: The end-to-end encryption keys are generated using the Key Pair Generator utility (createkey). For information on how to generate end-to-end encryption keys, see the following section of the documentation:

SQL Anywhere Server – Database Administration »
Administering Your Database »
Database administration utilities »
Key Pair Generator utility

Online:
http://dcx.sybase.com/index.php#http%3A%2F%2Fdcx.sybase.com%2F1100en%2Fdbadmin_en11%2Fda-dbutilities-s-4065300.html

例

RSA 暗号化を使用した TCP/IP 接続

下記は、暗号化タイプが RSA のエンドツーエンド暗号化を有効にした Mobile Link サーバを TCP/IP で接続する例を示したものです。

```
mlsrv11 … –x
```

```
tcpip{port=2439;e2ee_type=RSA;e2ee_private_key=
rsaprivate.pem;e2ee_private_key_password=pwd}
```

Mobile Link クライアントでは、拡張オプション・スイッチ (-e) を使用して、以下の接続プロトコル・オプションを指定できます。

```
dbmlsync … –e "ctp=tcpip;adr='
=localhost;port=2439;e2ee_type=rsa;e2ee_public_key=rsapublic.pem'"
```

Ultra Light クライアントでは、以下の接続プロトコル・オプションを指定できます。

```
info.stream = "tcpip";
info.stream_parms =
"e2ee_type=rsa;e2ee_public_key=rsapublic.pem";
```

暗号化タイプが RSA のエンドツーエンド暗号化と TLS による RSA 暗号化を使用した TCP/IP 接続

下記は、暗号化タイプが RSA のエンドツーエンド暗号化を有効にした Mobile Link サーバを TCP/IP で接続するとともに、TLS による RSA 暗号化によって Mobile Link データ・ストリームを暗号化する例を示したものです。

```
mlsrv11 –x tls{port=2439;tls_type=rsa;identity=
id.pem;identity_password=pwd;e2ee_type=RSA;e2ee_private_k
ey=rsaprivate.pem;e2ee_private_key_password=pwd}
```

Mobile Link クライアントでは、拡張オプション・スイッチ (-e) を使用して、以下の接続プロトコル・オプションを指定できます。

```
dbmlsync -e "
ctp=tls;adr='host=localhost;port=2439;tls_type=rsa;truste
d_certificates=certs.pem;certificate_company=Sybase;certi
ficate_unit=Sybase;certificate_name=Sybase;e2ee_type=rsa;
e2ee_public_key=rsapublic.pem'"
```

Ultra Light クライアントでは、以下の接続プロトコル・オプションを指定できます。

```
info.stream = "tls";
info.stream_parms = "
tls_type=rsa;trusted_certificates=certs.crt;e2ee_type=rsa
```

```
;e2ee_public_key=rsapublic.pem";
```

暗号化タイプが RSA のエンドツーエンド暗号化と TLS による ECC 暗号化を使用した HTTPS 接続

下記は、暗号化タイプが RSA のエンドツーエンド暗号化を有効にした Mobile Link サーバを HTTPS で接続するとともに、TLS による ECC 暗号化によって Mobile Link データ・ストリームを暗号化する例を示したものです。

```
mlsrv11 –x
https{port=2439;tls_type=ecc;identity=id.pem;identity_pas
sword=pwd;e2ee_type=rsa;e2ee_private_key=rsaprivate.pem;e
2ee_private_key_password=pwd}
```

Mobile Link クライアントでは、拡張オプション・スイッチ (-e) を使用して、以下の接続プロトコル・オプションを指定できます。

```
dbmlsync –e
"ctp=https;adr='host=localhost;port=2439;tls_type=ecc;tru
sted_certificates=certs.pem;certificate_company=Sybase;ce
rtificate_unit=Sybase;certificate_name=Sybase;e2ee_type=r
sa;e2ee_public_key=rsapublic.pem'"
```

Ultra Light クライアントでは、以下の接続プロトコル・オプションを指定できます。

```
info.stream = "https";
info.stream_parms = "
tls_type=ecc;trusted_certificates=certs.crt;e2ee_type=rsa
;e2ee_public_key=rsapublic.pem";
```

まとめ

このマニュアルでは、SQL Anywhere 11 に新たに搭載された Mobile Link 機能の 1 つであるエンドツーエンド暗号化機能について説明しました。この機能には、ネットワーク全体や WAP ギャップの中で RSA または ECC 暗号化を使用し、Mobile Link 同期データ・ストリームを保護できるというメリットがあります。したがって、この機能を利用すれば、仲介役が TCP/IP、HTTP、HTTPS のトランスポート・プロトコルを使用してデータにアクセスする可能性を排除することができます。

また、既存の TLS に影響を与えないエンドツーエンド暗号化機能は、Mobile Link データ・ストリームを暗号化できる特別なセキュリティ・オプションもサポートしています。なお、この暗号化機能で暗号化された

データ・ストリームは、TLS で再度暗号化できます。

法的注意