ICS 29.240.30
F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.4—2010/IEC TS 62351-4:2007

电力系统管理及其信息交换 数据和通信安全 第4部分:包含MMS的协议集

Power systems management and associated information exchange—Data and communications security—Part 4:Profiles including MMS

(IEC TS 62351-4:2007,IDT)

2010-11-10 发布　　2011-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

国际电工委员会57技术委员会(IEC TC 57)对电力系统控制的相关数据和通信安全制定了IEC 62351《电力系统管理及其信息交换　数据和通信安全》标准。我们采用IEC 62351，编制了GB/Z 25320指导性技术文件，主要包括以下部分：

——第1部分：通信网络和系统安全　安全问题介绍；

——第2部分：术语；

——第3部分：通信网络和系统安全　包含TCP/IP的协议集；

——第4部分：包含MMS的协议集；

——第5部分：IEC 60870-5及其衍生标准的安全；

——第6部分：DL/T 860的安全；

——第7部分：网络和系统管理的数据对象模型；

——第8部分：电力系统管理的基于角色访问控制。

本部分等同采用IEC TS 62351-4:2007《电力系统管理及其信息交换　数据和通信安全　第4部分：包含MMS的协议集》(英文版)。

本部分由中国电力企业联合会提出。

本部分由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本部分起草单位：中国电力科学研究院、华东电网有限公司、国家电力调度通信中心、国网电力科学研究院、福建省电力有限公司、华中电网有限公司、辽宁省电力有限公司。

本部分主要起草人：杨秋恒、李根蔚、许慕樑、邓兆云、南贵林、韩水保、曹连军、袁和林、林为民。

本指导性技术文件仅供参考。有关对本指导性技术文件的建议或意见，向国务院标准化行政主管部门反映。

引　言

计算机、通信和网络技术当前已在电力系统中广泛使用。通信和计算机网络中存在着各种对信息安全可能的攻击，对电力系统的数据及通信安全也构成了威胁。这些潜在的可能的攻击针对着电力系统使用的各层通信协议中的安全漏洞及电力系统信息基础设施的安全管理的不完善处。

为此，我们采用国际标准制定了GB/Z 25320《电力系统管理及其信息交换　数据和通信安全》，通过在相关的通信协议及在信息基础设管理中增加特定的安全措施，提高和增强电力系统的数据及通信的安全。

电力系统管理及其信息交换 数据和通信安全 第4部分:包含MMS的协议集

1 范围和目的

1.1 范围

为了对基于GB/T 16720(ISO 9506)制造报文规范(Manufacturing Message Specification,MMS)的应用进行安全防护,GB/Z 25320的本部分规定了过程、协议扩充和算法。其他IEC TC 57标准如需要以安全的方式使用MMS,可以引用本部分作为其规范性引用文件。

本部分描述了在使用GB/T 16720(ISO/IEC 9506)制造业报文规范MMS时应实现的一些强制的和可选的安全规范。

注:在IEC TC 57范围内,有两个标准DL/T 860.81—2006(IEC 61850-8-1)及GB/T 18700(IEC 60870-6)会受到影响。

为了保护使用MMS传递的信息,本部分包含一组由这些引用标准所使用的规范。其建议是基于为传送MMS信息所使用的特定通信协议集的协议。

DL/T 860.81—2006(IEC 61850-8-1)和GB/T 18700(IEC 60870-6)在第7层的面向连接机制中使用了MMS。这些标准中每一个均是在OSI协议集或TCP协议集上使用。

1.2 目的

本部分的初期读者预期是制定或使用IEC TC 57协议的工作组成员。为了使本部分描述的措施有效,对于那些使用GB/T 16720的协议,协议本身的规范就必须采纳和引用这些措施。本部分就是为了使得能那样做而编写的。

本部分的后续读者预期是实现这些协议的产品的开发人员。

本部分的某些部分也可以被管理者和行政人员使用,以理解该工作的用途和需求。

2 规范性引用文件

下列文件中的条款通过GB/Z 25320的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 16720(所有部分) 工业自动化系统 制造报文规范(ISO 9506)

GB/T 18700(所有部分) 远动设备及系统(IEC 60870-6)

GB/Z 25320.1 电力系统管理及其信息交换 数据与通信安全 第1部分:通信网络和系统安全 安全问题介绍(GB/Z 25320.1—2010,IEC TS 62351-1:2007,IDT)

GB/Z 25320.3 电力系统管理及其信息交换 数据和通信安全 第3部分:通信网络和系统安全 包括TCP/IP的协议集(GB/Z 25320.3—2010,IEC 62351-3:2007,IDT)

IEC TS 62351-2 电力系统管理及其信息交换 数据和通信安全 第2部分:术语(Power systems management and associated information exchange—Data and communications security—Part 2:Glossary of terms)

ISO/IEC 9594-8:2005/ITU-T X.509建议:2005 信息技术 开放系统互连 目录:公钥和属性

证书框架(ISO/IEC 9594-8:2005/ITU-T Recommendation X.509:2005, Information technology—Open Systems Interconnection—The Directory:Public-key and attribute certificate frameworks)

RFC 1006 版本 3 在 TCP 之上的 ISO 传输服务(ISO Transport Service on top of the TCP Version:3)

RFC 2246 版本 1.0 传输层安全协议(TLS)(The TLS Protocol, Version 1.0)

RFC 2313 版本 1.5 PKCS #1:RSA 加密(PKCS #1:RSA Encryption Version 1.5)

RFC 3447 版本 2.1 公钥密码标准(PKCS)#1:RSA 密码技术规范[Public-Key Cryptography Standards(PKCS) #1:RSA Cryptography Specifications Version 2.1]

3 术语和定义

IEC 62351-2 中给出的以及下列的术语和定义适用于 GB/Z 25320 的本部分。

3.1

双边协议 bilateral agreement

两个控制中心之间关于被访问的数据元素及其访问方法的协议。

[GB/T 18700.1—2002,定义 3.3]

3.2

双边表 bilateral table

双边协议的计算机表示法。具体的表示方法是当地的事。

[GB/T 18700.1—2002,定义 3.4]

4 本部分涉及的安全问题

4.1 应用和传输协议集的安全

在本部分中规定的通信安全应按应用协议集和传输协议集讨论:

- 应用协议集(A-Profile):规定了 OSI 参考模型 5～7 层整套的协议和要求;
- 传输协议集(T-Profile):规定了 OSI 参考模型 1～4 层整套的协议和要求。

在 TC 57 涉及的通信协议中已规定了(1) A-Profile 和(2) T-Profile。本部分规定这些已确定的协议集的安全扩展,见图 1。

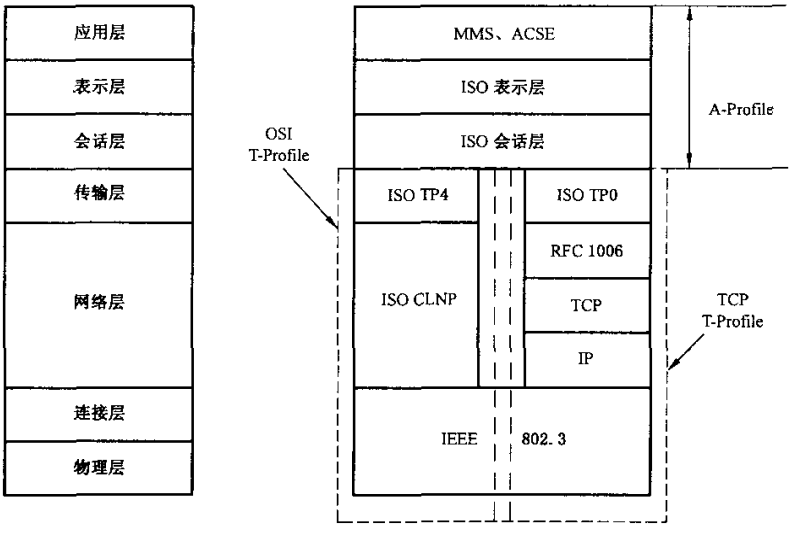

图 1 应用和传输协议集

4.2 应对的安全威胁

对安全威胁和攻击方法的讨论详见 GB/Z 25320.1。

如不用加密,则本部分需应对的特定威胁有:

未经授权的访问信息。

如用 GB/Z 25320.3,则本部分需应对的特定威胁有:

- 通过消息层面认证和消息加密,应对未经授权的访问信息;
- 通过消息层面认证和消息加密,应对未经授权的修改(篡改)或窃取信息。

4.3 应对的攻击方法

通过适当实现本部分的规范或建议,应对以下的安全攻击方法。以下内容未包含通过 GB/Z 25320.3 应对的攻击方法。在不用 GB/Z 25320.3 的情况下,所应对的威胁仅限于关联建立时的防护。

- 中间人:通过本部分规定的消息鉴别码(Message Authentication Code)机制应对该威胁;
- 篡改或破坏消息完整性:通过为创建本部分规定的认证机制而使用的算法应对该威胁;
- 重放:通过本部分规定的特定处理状态机应对该威胁。

5 应用协议集(A-Profile)安全

以下条款详细说明了声称符合于本部分的实现应支持的应用协议集(A-Profile)。

5.1 MMS

MMS 的实现必须提供配置和使用安全协议集能力的某些机制。通常需要提供以下机制:

- 配置证书信息和把证书信息与访问认证绑定起来的机制(例如:双边表);
- 为实现的访问控制机制,配置呼入关联的可接受协议集的机制。建议提供以下选择:
  ——DON' T_CARE:安全协议集或非安全协议集都可以建立 MMS 关联。
  ——NON_SECURE:必须使用非安全协议集才能建立 MMS 关联。
  ——SECURE:必须使用安全协议集才能建立 MMS 关联。
- 为发起 MMS 关联,配置所用协议集的机制。建议提供以下选择:
  ——NON_SECURE:必须使用非安全协议集才能建立 MMS 关联。
  ——SECURE:必须使用安全协议集才能建立 MMS 关联。
- 传送或校验关联参数的机制。这些参数宜包括:表示层地址、所用协议集的标志(例如,安全或非安全协议集),以及 ACSE(关联控制服务元素)认证参数。如果像本部分阐述的那样,已经协商把安全传输层作为 MMS 关联的一部分[1],那么应保留"secure profile"("安全协议集")的使用标志。
  应使用该关联参数信息且连同配置的 MMS 期望的关联值,以确定是否应建立 MMS 关联。确定实际接受的实体是当地问题。

上述讨论的配置参数的改变并不要求为使配置改变生效需终止所有的 MMS 关联,这是强制的要求。

对于因安全违例而被拒绝的被拒关联,强烈建议 MMS 实现应记录与该种被拒关联相关的事件和信息。

5.2 记录

重要的是,一定要把与安全有关的违例记录到一个单独的日志文件中。该日志文件的内容本质上是禁止操作的(例如,修改信息或删除信息)。实现者应力求保存足够多的信息,这样就便于安全审计和诉讼。此建议的实际实现是当地问题。

---

1) 为达到更强认证,在安全协议集或非安全协议集上都可使用 ACSE 认证。

5.3 关联控制服务元素(ACSE)

5.3.1 对等实体认证

对等实体的认证应发生在关联建立时。对 ACSE(关联控制服务元素)的 AARQ(关联认证请求)报文和 AARE(关联认证响应)报文,应在 AARQ 的 PDU(协议数据单元)的认证功能单元(认证 FU)的 calling-authentication-value(呼叫-认证-值)字段和 AARE 的 PDU 的认证功能单元的 responding-authentication-value(应答-认证-值)字段中携带认证信息。

在使用 ACSE 安全时为了包括认证 FU,对于认证 FU 的 sender-ACSE-requirements(发送者-关联控制服务元素-请求)和 responder-ACSE-requirements(应答者-关联控制服务元素-请求)字段的比特串应是 DEFAULTED;否则,不使用 ACSE 安全时,这些比特串虽仍应是 DEFAULTED 却是为了不包括认证 FU。这提供了向后兼容性。

Calling-authentication-value 和 responding-authentication-value 字段是 authentication-value(认证-值)类型,该类型作为 CHOICE 在 GB/T 16687(ISO 8650)中进一步定义。该 authentication-value 的 CHOICE 应是 EXTERNAL(外部的)。为此 EXTERNAL 使用了抽象句法,所以,表示层的上下文应包括对该抽象句法的引用。

为表示传递的 authentication-value(认证值)字段的格式,应使用 ACSE 的 mechanism-name(机制名)字段。AARQ 和 AARE 的 mechanism-name 字段定义应是:

应在 ACSE 的认证 FU 的 authentication-value 字段中携带 ICCP 的认证值(如下所述)。在要求对等实体认证时,该认证值将会被使用。该值应按"external"携带,按 ACSE 的 authentication-value 形式语法表达式(ACSE authentication-value production)(已复制在下面)以 SingleASN1 Type 类型定义。

注:以下形式语法表达式是从 GB/T 16687(ISO 8650)复制的,仅供参考。

```
Authentication-value::= CHOICE {
        charstring   [0] IMPLICIT GraphicString,
        bitstring    [1] IMPLICIT BIT STRING,
        external     [2] IMPLICIT EXTERNAL,
        other        [3] IMPLICIT SEQUENCE {other-mechanism-name
                             MECHANISM-NAME. &id({ObjectSet}),
                             other-mechanism-value
                             MECHANISM-NAME. &Type
              }
        }
        STASE-MMS-Authentication-value {iso member-body usa(840) ansi-tl-259-1997(0)
        stase(1) stase-authentication-value(0) abstractSyntax(1) version1(1)}
        DEFINITIONS IMPLICIT TAGS::= BEGIN
        -- EXPORTS everything
        IMPORTS
        SenderId, ReceiverId, Signature, SignatureCertificate
        FROM ST-CMIP-PCI {iso member-body usa (840) ansi-tl-259-1997 (0) stase(1) stasepci(1)
        abstractSyntax(4) version1(1)};
        MMS_Authentication-value::= CHOICE{
                certificate-based [0] IMPLICIT SEQUENCE {
                authentication-Certificate [0] IMPLICIT &SignatureCertificate,
                time [1] IMPLICIT GENERALZEDTIME,
                signature [2] IMPLICIT &SignedValue
```

},

...}

END

&SignatureCertificate

SignatureCertificate::= OCTET STRING—字节数应为 8 192 八位位组的最小的最大(minimum-maximum)字节数。

SignatureCertificate(签名证书)的 OCTET STRING(八位位组串)内容应按照基本编码规则(Basic Encoding Rule)编码的 X.509 证书(在 CMIP 中规定)。证书的交换应是双向的,且应提供来自某个已配置且可信的证书机构的个体证书。如果以上条件任何一项不符合,则连接应被适当地终止。

个体证书的身份证明至少应是基于证书的 Subject(主体)。

为了达到证书的互操作性,必须为 ACSE 交换的证书设定最大允许字节数。这个字节数应限于 8 192 个八位位组的最大编码字节数。

是否能接受更大的证书,这是当地问题。

如果证书的字节数超过最小的最大值(minimum-maximum)(例如 8 192)或当地的最大值,则应拒绝该连接且应拆除连接。

&SignedValue

SignedValue(签名值)的值按 PKCS#1 Version 2 规定应是签署的 time 字段的值。该值是 GENERALZEDTIME 编码串,但不包含 ASN1 的标记或长度。这个值在该规范中应是经 RSA 签名算法签署。应支持 1 024 比特的密钥长度作为最小的最大值(minimum-maximum)。

在 RFC 2313 中的数字签名(DigitalSignature)定义中规定了 SignedValue 的定义:

"作为数字签名,首先将要签名的内容用消息/摘要算法(例如 MD5)简化为消息摘要,然后包含消息摘要的八位位组串用该内容签名者的 RSA 私钥加密。根据 PKCS #7 的语法将内容和加密后的消息摘要一起表示而生成一个数字签名。"

注:在该定义中对 MD5 的引用并不是规范性的,这是 RFC 2313 引用文本中所给的例子。在下一段落中规定的实际算法是 SHA1。

RFC 3447(PKCS#1 规范 Version 2)规定以 RSASSA-PKCS1-v1_5 作为签名算法。该算法是声称符合本部分的具体实现都应使用的算法。RFC 3447 的使用应限于与 PKCS Version 1.5(RFC 2313)兼容的那些能力。哈希算法应是 SHA1。

Time

该参数应是创建 authentication-value 的时间,用 GENERALIZEDTIME 格式表示的格林威治时间(GMT)值。

该时间的精度是一个当地问题,但应尽可能的精确。在调用 MMS 的 Intiate.Request(启动请求)服务、Intiate.Response(启动应答)服务期间或在这些服务的 ACSE 的 PDU 编码期间,确定该时间参数值都是同等有效的。

5.3.2 关联认证请求(AARQ)

AARQ 的发送者应该对适当的 ACSE 的 AuthenticationMechanism 和 AuthenticationValue 字段进行编码并应通过使用 Presentation-Connect(表示层-连接)服务发送 AARQ。

AARQ-indication(AARQ-指示)原语的接收者应使用 AuthenticationMechanism 和 AuthenticationValue 字段去校验签名值。如果解码后的签名值不等于 time 字段的值,则应导致接收者发出 P-ABORT(表示层-异常终止)原语;如果 time 字段值与当地时间之差大于 10 min[2],则也应导致接收者发出 P-ABORT 原语。

如果该 AARQ 的接收者在最近 10 min 之内已经接收到包含相同签名值的 AARQ,则应导致接收

2) 这意味着存在一个 10 min 的脆弱性窗口,在此期间相同的签名值可能被攻击者利用。

者发出 P-ABORT 原语。

如果签名值没有导致 P-ABORT，则签名值及其他的安全参数就应传送给 ACSE 的用户（例如 MMS 或 TASE.2 或当地的应用）。传送这些参数的方法是当地问题。

5.3.3 关联认证响应（AARE）

AARE 的发送者应该对适当的 ACSE 的 AuthenticationMechanism 和 AuthenticationValue 字段进行编码并应通过使用 Presentation-Connect 服务发送 AARE。

AARE-indication 原语的接收者用 AuthenticationMechanism 和 AuthenticationValue 字段去校验签名值。如果解码之后的签名值不等于 time 字段的值，应导致接收者发出 P-ABORT 原语；如果 time 字段值与本地时间之差大于 10 min[3)]，也应导致接收者发出 P-ABORT 原语。

如果该 AARE 的接收者在最近 10 min 之内已经接收到包含相同签名值的 AARE，则应导致接收者发出 P-ABORT 原语。

如果签名值没有导致 P-ABORT，则应将签名值及其他安全参数传送给 ACSE 的用户（例如 MMS 或 TASE.2 或当地的应用）。传送这些参数的方法是当地问题。

6 传输协议集（T-Profile）安全

6.1 TCP 传输协议集

6.1.1 与本部分的一致性

声称符合本部分的实现应支持对 TCP T-Profile 的安全防护。

6.1.2 TCP 传输协议集中使用 TLS

TCP T-Profile 的安全建议并不试图为 TCP、IP 或 Ethernet 规定安全建议，而是本部分的各规范规定了如何适当地使用传输层安全协议（Transport Layer Security TLS）及对 RFC 1006 进行安全防护。

TCP T-Profile 嵌入了安全防护造成使用 TLS（由 RFC 2246 规定）提供在 RFC 1006 之前的加密和节点认证。

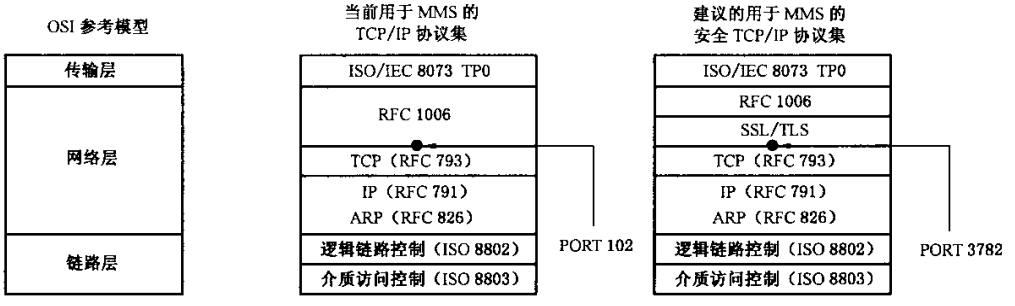

图 2 非安全和安全的 TCP T-Profile

图 2 展示了两个相关的 TCP T-Profile，一个是由互联网工程任务组（IETF）规定的标准的 RFC 1006 T-Profile，即非安全的 RFC 1006 T-Profile，另外一个是在本部分内所规定的安全的 RFC 1006 T-Profile。

6.1.3 传输协议 0 类（TP0）

6.1.3.1 强制的最大长度

TP0 规定了 TPDU（传输层协议数据单元）的最大字节数。建议实现用表 1 确保 RFC 1006 的长度不超过最大字节数。关于对 RFC 1006 字节数不正确的 TPDU 进行处理的问题是当地问题。

---

3) 这意味着存在一个 10 min 的脆弱性窗口，在此期间相同的签名值可能被攻击者所利用。

表 1 TP0 最大字节数

OSI TP0 原语	RFC 1006 头部	ISO TP0 LI 字段		ISO TP0 用户数据		RFC 1006 长度范围	
	字节	最小	最大	最小	最大	最小	最大
CR	4	7	254	0	0	11	258
CC	4	7	254	0	0	11	258
DR	4	7	254	0	0	11	258
DC	4	7	254	0	0	11	258
DT	4	3	3	1	2048 注	8	2056
ER	4	5	254	0	0	9	259
ED	由于 TP0 的限制，不允许						
AK	由于 TP0 的限制，不允许						
EA	由于 TP0 的限制，不允许						
RJ	由于 TP0 的限制，不允许						
注：基于 CR/CC 交换时协商的最大字节数。128 个八位位组是允许的最小字节数。							

6.1.3.2 对 TP0 不支持的 TPDU 的响应

建议不理会接收到的 ED、AK、EA 或 RJ 原语的 TPDU。

6.1.3.3 传输层选择段

MMS 的国际标准化协议集(International Standardized Profiles ISP)规定传输层选择段(Transport Selector TSEL)应具有 32 个八位位组的最大字节数。然而根据 ISO/IEC 8073，参数化的选择段可以具有 255 个八位位组的长度。

TSEL 的长度若大于 32 个八位位组，应导致接收该 TSEL 的实现将该连接异常终止。

6.1.4 RFC 1006

在安全或非安全 T-Profile 中使用 RFC 1006 时，建议对 RFC 1006 实现作以下增强。

6.1.4.1 版本号

当地实现应不理会 RFC 1006 的 version 字段的值。继续对 OSI 的 TPDU 进行当地处理，好像该字段值是 3 一样。

6.1.4.2 长度

RFC 1006 的 length 字段应限制为不大于 2 056 个八位位组的值。这个长度对应于允许的最大 TP0 的 TPDU(如：2 048 个八位位组)。

对大于 2 056 个八位位组的长度进行处理是当地问题；然而，强烈建议拆除该连接。

6.1.4.3 保持存活

声称符合于本部分的实现应使用保持存活(TCP-KEEPALIVE)功能。其超时参数应设置为大约 1 min 或少些。

6.1.5 TLS 要求

6.1.5.1 TCP 端口的使用

按 RFC 1006 规定，非安全 T-Profile 应使用 TCP 的 102 端口。

声称符合于本部分的实现应使用 TCP 的 3782 端口，以表明使用了安全的 TCP T-Profile。

6.1.5.2 同时支持

以下需求适用于声称支持一个以上的同时的 MMS 关联的实现。对于这样的实现，通过安全及非安全 T-Profile 同时进行通信应是可能的。

6.1.6 TLS 的使用

应按 GB/Z 25320.3 规定使用传输层安全协议(TLS)。

6.1.6.1 TLS 的停用

实现应允许暂时停用 TLS。

6.1.6.2 密码再协商

如果自上次再协商之后已发送 5 000 个 ISO TPU 或已超过 10 min,声称符合于本部分的实现应支持按最小的最大(minimum-maximum)密钥长度的密钥再协商。

6.1.6.3 证书长度

声称符合于本部分的实现应支持 8 192 个八位位组的最小的最大(minimum-maximum)证书字节数。是否支持更大的证书是当地问题。

实现接收到大于它所能支持字节数的证书,则该实现应终止这连接。

6.1.6.4 证书撤销

撤销证书的缺省评估周期应为 12 h。该评估周期应是可配置的。

当用于建立连接的证书之一被撤消,声称符合于本部分的实现应终止这连接。

6.1.6.5 强制的和建议的密码套件

声称符合于本部分的所有实现应至少支持 TLS_DH_DSS_WITH_AES_256_SHA。

引用本部分的其他标准可以增加另外的强制密码套件。

建议考虑使用表 2 所列的 TLS 密码套件。

表 2 建议的密码套件组合

密钥交换		加密	哈希
算法	签名		
TLS_RSA_	—	WITH_RC4_128_	SHA
TLS_RSA_	—	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_AES_128_	SHA
TLS_DH_	DSS_	WITH_AES_256_	SHA
TLS_DH_	—	WITH_AES_128_	SHA
TLS_DH_	—	WITH_AES_256_	SHA

注:基于已配置的许可或现有的密码套件,TLS 的协商机制选择为特定连接使用的实际密码套件。

6.2 OSI 的传输协议集

OSI T-Profile 的安全超出本部分范围。

6.3 证书机构支持

为支持四个不同证书机构所提供的证书,声称符合于本部分的实现应支持最小的最大(minimum-maximum)证书字节数能力。

7 一致性

7.1 一般的一致性

与本部分的一致性应由第 5 章和第 6 章的实现决定。

此外，应提供以下支持密码套件表：

- 强制的：应支持的；
- 可选的：可支持的。

表 3 支持的密码套件

密钥交换		加密	哈希	支持		
算法	签名			可互操作	出口限制	支持
TLS_RSA_	—	WITH_RC4_128_	SHA	可选	注 1	—
TLS_RSA_	—	WITH_3DES_EDE_CBC_	SHA	可选	注 1	—
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA	可选	注 1	—
TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA	可选	注 1	—
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA	可选	注 1	—
TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA	可选	注 1	—
TLS_DHE_	DSS_	WITH_AES_128_	SHA	可选	注 1	—
TLS_DH_	DSS_	WITH_AES_256_	SHA	可选	注 1	—
TLS_DH_	—	WITH_AES_128_	SHA	可选	注 1	—
TLS_DH_	—	WITH_AES_256_	SHA	必备	注 1，注 2	—

注 1：在出口限制基础上，应支持至少一种密码套件。如不支持 TLS_DH_WITH_AES_256_SHA，TLS 互操作性也许就不可能。

注 2：如没有声明支持，实现就应提供一份禁止该密码套件出口的出口限制拷贝。如果且只有如果出口限制不准许任何途径出口，才不应支持该套件。如果不支持该套件，作为补充，实现应清楚地以文件说明是因遵守出口限制所致。该文件同样应详细说明不能支持的互操作要求或基本规范要求。该文件的样本应作为用户文件的一部分提供，这样用户就能够理解由于出口限制的原因，实现也许不是能互操作的。

7.2 GB/T 18700 TASE.2 安全的一致性

声称支持标准化安全防护的 GB/T 18700(IEC 60870-6)实现应符合本部分。

参 考 文 献

[1] GB/T 16687 信息技术 开放系统互连 面向连接的联系控制服务元素协议(ISO 8650,IDT)

[2] GB/T 16688 信息技术 开放系统互连 联系控制服务元素服务定义(ISO 8649,IDT)

[3] GB/T 16720.1—2005 工业自动化系统 制造报文规范 第1部分:服务定义(ISO 9506-1:2003,IDT)

[4] GB/T 16720.2—2005 工业自动化系统 制造报文规范 第2部分:协议规范(ISO 9506-2:2003,IDT)

[5] ISO/ISP 14226-1:1996 工业自动化系统 国际标准化协议集 AMM11:MMS普通的应用基础协议集 第1部分:MMS所使用的ACSE、表示层及会话层的规范(Industrial automation systems—International Standardized Profile AMM11:MMS General Applications Base Profile—Part 1:Specification of ACSE,Presentation and Session protocols for use by MMS)

[6] ISO/ISP 14226-2:1996 工业自动化系统 国际标准化协议集 AMM11:MMS普通的应用基础协议集 第2部分:公共的MMS要求(Industrial automation systems—International Standardized Profile AMM11:MMS General Applications Base Profile—Part 2:Common MMS requirements)

[7] ISO/ISP 14226-3:1996 工业自动化系统 国际标准化协议集 AMM11:MMS普通的应用基础协议集 第3部分:特殊的MMS要求(Industrial automation systems—International Standardized Profile AMM11:MMS General Applications Base Profile—Part 3:Specific MMS requirements)

[8] FIPS-180-1 安全的哈希标准(Secure Hash Standard)

[9] RFC 3174 US的安全哈希算法1(SHA1)[US Secure Hash Algorithm 1 (SHA1)]

[10] RFC 3280 因特网X.509 PKI证书以及证书撤销列表(CRL)格式(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile)