ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33746.2—2017

近场通信(NFC)安全技术要求
第2部分:安全机制要求

**Technical specification of NFC security—
Part 2:Security mechanism requirements**

(ISO/IEC 13157-2:2010,Information technology—
Telecommunications and information exchange between
systems—NFC Security—Part 2:Security mechanism requirements,
NFC-SEC cryptography standard using ECDH and AES,MOD)

2017-09-07 发布　　2018-01-01 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

GB/T 33746《近场通信(NFC)安全技术要求》分为以下 2 部分：

——第 1 部分：NFCIP-1 安全服务和协议；

——第 2 部分：安全机制要求。

本部分为 GB/T 33746 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用 ISO/IEC 13157-2：2010《信息技术　系统间通信及信息交互 NFC 安全　第 2 部分：安全机制要求，使用 ECDH 和 AES 的密码标准》。

本部分与 ISO/IEC 13157-2：2010 的技术性差异及其原因如下：

——标准的英文名称修改为 Technical specification of NFC security—Part 2：Security mechanism requirements；

——增加了 3 个规范性引用文件；

——增加了 5 个缩略语；

——删除原资料性附录 C，增加了 2 个规范性附录 C 和附录 D；

——将 AES 替换为符合国家密码管理相关规定的密码算法。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：工业和信息化部电信研究院、西安西电捷通无线网络通信股份有限公司、国家射频识别产品质量监督检验中心、中国物品编码中心。

本部分主要起草人：孙倩、张琳琳、杨军、杜志强、胡亚楠、鄢若韫、姜国强、李志敏、罗艳。

引　言

本部分的使用者是通信行业的生产企业、检测机构和科技机构。

本文件的发布机构提请注意，声明符合本文件时，可能涉及附录C与“一种实体双向鉴别方法”、附录D与“一种基于对称密码算法的实体鉴别方法及系统”等相关的专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路68号西安软件园秦风阁A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

请注意除上述专利外，本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

近场通信(NFC)安全技术要求
第2部分:安全机制要求

1 范围

GB/T 33746的本部分规定了协议标识符PID为01的消息内容和加密方法。本部分的密码机制是使用SM2密钥交换协议作为密钥协定协议以及SM4分组密码算法用于数据加密和完整性保护。

本部分适用于NFC安全服务建立中的安全机制的要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 17964—2008 信息安全技术 分组密码算法的工作模式

GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

GB/T 33746.1—2017 近场通信(NFC)安全技术要求 第1部分:NFCIP-1安全服务和协议(ISO/IEC 13157-1:2010,MOD)

GM/T 0002—2012 SM4分组密码算法

GM/T 0003—2012 SM2椭圆曲线公钥密码算法

ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第3部分:使用数字签名技术的机制 补篇1(Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—Amendment 1)

ISO/IEC 18092:2004 信息技术 系统间远程通信和信息交换 近场通信 接口和协议NFCIP-1[Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol(NFCIP-1)]

ISO/IEC 20009-2:2013 信息技术 安全技术 匿名实体鉴别 第2部分:采用群组公钥技术的机制(Information technology—Security techniques—Anonymous entity authentication—Part 2:Mechanisms based on signatures using a group public key)

3 术语和定义

GB/T 33746.1—2017界定的术语和定义适用于本文件。

4 约定和记法

4.1 级连

A‖B表示字段A和字段B的级联:B内容在A内容之后。

4.2 十六进制数字

(XY)代表XY的十六进制数(即以16为基数),每对字符编码为一个字节。

5 缩略语

下列缩略语适用于本文件。

A	发送者	(Sender)
AA/BB	NFC-SEC 实体对	(NFC-SEC peer entity)
B	接收者	(Recipient)
d_A	发送者的 EC 私钥	(Sender's private EC key)
d_B	接收者的 EC 私钥	(Recipient's private EC key)
D_A	发送者的证书私钥	(Sender's certificate private key
D_B	接收者的证书私钥	Recipient's certificate)(private key)
DataLen	用户数据的长度	(Length of the User Data)
EC	椭圆曲线	(Elliptic Curve)
ECDH	椭圆曲线 Diffie-Hellman 密码算法	(Elliptic Curve Diffie-Hellman)
EncData	加密数据	(Encrypted data)
G	EC 的基点	(The base point on EC)
ID_A	发送者 nfcid3	(Sender nfcid3)
ID_B	接收者 nfcid3	(Recipient nfcid3)
ID_R	任意接收者识别码(例如 ID_B)	(Any Recipient identification number (e.g. IDB))
ID_S	任意发送者识别码(例如 ID_A)	(Any Sender identification number (e.g. IDA))
IV	初始向量	(Initial Vector)
K	密钥	(Key)
KDF	密钥导出函数	(Key Derivation Function)
KE	加密密钥	(Encryption Key)
KI	完整性密钥	(Integrity Key)
MAC	消息鉴别码	(Message Authentication Code)
Mac_A/Mac_B	发送者/接收者完整性保护值	(Integrity protection value of Sender/Recipient)
$MacTag_A$	发送者密钥确认标识	(Key confirmation tag from Sender)
$MacTag_B$	接收者密钥确认标识	(Key confirmation tag from Recipient)
MK	主密钥	(Master Key)
NA/NB	发送者/接收者产生的随机数	(Nonce generated by Sender/Recipient)
NAA/NBB	NFC-SEC 实体对产生的随机数	(Nonce generated by the pair of NFC-SEC entities)
NEAU	NFC 实体鉴别	(NFC Entity Authentication)
$Nonce_S$	发送者的随机数	(Sender's nonce)
$Nonce_R$	接收者的随机数	(Recipient's nonce)
PID	协议标识符	(Protocol Identifier)
PK	公钥	(Public Key)
PK_R	接收者公钥	(Recipient's Public Key)
PK_S	发送者公钥	(Sender's Public Key)

PRNG	伪随机数生成器	(Pseudo Random Number Generator)
QA/QB	发送者/接收者压缩临时公钥	(Compressed temporary public key of Sender/Recipient)
Q_A/Q_B	发送者/接收者解压临时公钥	(Decompressed temporary public key of Sender/Recipient)
RNG	随机数生成器	(Random Number Generator)
SharedSecret	共享秘密	(Shared secret)
TePA	三元对等架构	(Tri-element Peer Architecture)
TePA-AC	基于三元对等架构的访问控制	(TePA-based Access Control)
UserData	NFC-SEC 用户数据	(NFC-SEC User data)
z	共享秘密的无符号整数表示	(Unsigned integer representation of the Shared Secret)
Z	z 的字节串表示	(Octet string representation of z)

注：第 9 章和第 10 章中使用的以上未列出的英文缩写不是缩略语，而是公式或原语参数。

6 符合性

使用 NFC-SEC 安全机制(标识为 PID 1)的实现在声称符合本部分时还应满足 GB/T 33746.1 的要求。

NFC-SEC 安全服务的建立应通过 GB/T 33746.1 中定义的协议以及本部分中定义的安全机制来完成。

7 概要

本部分定义了 GB/T 33746.1 中 SSE(共享秘密服务)以及 SCH(安全通道服务)使用的安全机制。

为了在保证事先没有共享任何公用的秘密数据(“密钥”)的 NFC 设备之间的通信安全，使用公钥密码机制，即使用 SM2 密钥交换协议，在设备之间建立共享秘密。这个共享秘密被用来建立 SSE 和 SCH 服务。

本部分的附录 A 定义了 SM4-XCBC-PRF-128 和 SM4-XCBC-MAC-96 算法；附录 B 定义了字段长度；附录 C 和附录 D 定义了具备 NFC 实体鉴别 NEAU(NFC Entity Authentication)功能的安全机制，符合 ISO/IEC 9798-3:1998/Amd.1:2010 和 GB/T 28455—2012 的技术要求。

8 协议标识符(PID)

本部分应使用值为 1 的 1 字节协议标识符 PID。

9 原语

9.1 原语的特点概要

本章定义加密原语。第 11 章和第 12 章规定这些原语的使用。特点概要见表 1。

表 1　特点概要

支持的服务	SSE(见 GB/T 33746.1—2017) SCH(见 GB/T 33746.1—2017)
密钥协商	SM2 密钥交换协议
密钥导出函数(KDF)	SM4-XCBC-PRF-128
密钥确认	SM4-XCBC-MAC-96
数据加密	SM4-CTR IV Init:SM4-XCBC-PRF-128
数据完整性	SM4-XCBC-MAC-96
序列完整性	SN (见 GB/T 33746.1)
加密顺序	先加密(9.6)再计算 MAC(9.7)

9.2　密钥协商

9.2.1　概述

对等的 NFC-SEC 实体应该与使用 GM/T 0003—2012 中定义的密钥交换协议的秘密密钥达成一致,下面将对密钥交换协议原语做进一步的介绍。

9.2.2　曲线

应使用在 GM/T 0003—2012 中规定的 SM2 椭圆曲线公钥密码算法的曲线。

9.2.3　密钥对生成

密钥对的生成算法应符合 GM/T 0003—2012 的规定。

9.2.4　公钥验证

公钥应根据 GM/T 0003—2012 的公钥验证规定进行验证。

9.2.5　秘密密钥推导

密钥交换协议应根据 GM/T 0003—2012 的密钥交换协议及流程输出“有效的”共享秘密 z,否则输出“无效的”错误提示。

9.2.6　随机数

每个对等的 NFC-SEC 实体宜发送新的随机数和实体的公钥。

该随机数将更多的信息熵提供给由共享秘密 z 推导出来的密钥,便于密钥对的管理。

随机数的正确生成是实体的责任。

该实体应保证在协议期限生成的随机数有 96 位有效信息熵。在 NFC-SEC 传输过程中使用的随机数与之前使用的随机数没有密码关联性。

本部分规定使用国家密码管理局批准的随机数生成方法。

9.3　密钥导出函数

9.3.1　概述

这里规定了两个密钥导出函数(KDF),一个用于 SSE,另一个用于 SCH。

密钥导出函数应使用 A.1 中规定的 XCBC-PRF-128 模式下的 SM4 算法。

对于以下部分 KDF 为：

$$KDF(K,S)=SM4\text{-}XCBC\text{-}PRF\text{-}128_K(S)$$

用于 SCH 的随机源(随机数＋从 9.2.5 中获得的共享秘密 z)应不同于用于 SSE 的随机源。

9.3.2 SSE 的 KDF

用于 SSE 的 KDF 是：

$$MK_{SSE}=KDF\text{-}SSE(Nonce_S,Nonce_R,SharedSecret,ID_S,ID_R)$$

详细的 KDF-SSE 函数：

$$S=(Nonce_S[0..63]\parallel Nonce_R[0..63])$$

$$SKEYSEED=KDF\ (S,SharedSecret)$$

$$MK_{SSE}=KDF(SKEYSEED,S\parallel ID_S\parallel ID_R\parallel (01))$$

9.3.3 SCH 的 KDF

用于 SCH 的 KDF 是：

$$\{MK_{SCH},KE_{SCH},KI_{SCH}\}=KDF\text{-}SCH\ (Nonce_S,Nonce_R,SharedSecret,ID_S,ID_R)$$

详细的 KDF-SCH 函数：

$$S=(Nonce_S[0..63]\parallel Nonce_R[0..63])$$

$$SKEYSEED=KDF(S,SharedSecret)$$

$$MK_{SCH}=KDF\ (SKEYSEED,S\parallel ID_S\parallel ID_R\parallel (01))$$

$$KE_{SCH}=KDF\ (SKEYSEED,MK_{SCH}\parallel S\parallel ID_S\parallel ID_R\parallel (02))$$

$$KI_{SCH}=KDF\ (SKEYSEED,KE_{SCH}\parallel S\parallel ID_S\parallel ID_R\parallel (03))$$

9.4 密钥用途

每个推导出的密钥 MK_{SCH}，KE_{SCH}，KI_{SCH}和 MK_{SSE}应该仅用于表 2 规定的用途。

对于每一个 NFC-SEC 过程，密钥 MK_{SCH}，KE_{SCH}，KI_{SCH}和 MK_{SSE}应不同。

表 2 密钥用途

密钥	密钥描述	密钥用途
MK_{SCH}	SCH 的主密钥	作为安全信道密钥的验证
KE_{SCH}	SCH 的加密密钥	加密通过 SCH 发送的数据包
KI_{SCH}	SCH 的完整性保护密钥	通过 SCH 发送数据包的完整性保护
MK_{SSE}	SSE 的主密钥	共享秘密作为 SSE 的主密钥，用于传递给上层时使用并且可用于密钥验证

9.5 密钥确认

9.5.1 概述

当使用在 9.3 中规定的一个 KDF 过程生成一个密钥时，对等的 NFC-SEC 实体都要检查是否双方确实拥有相同的密钥。每一个实体应产生一个在 9.5.2 规定的密钥确认标识并且应将其发送到对等实体。接收实体应根据 9.5.3 中的规定来核实密钥确认标识。

用于密钥确认 MAC(MacTag)应为 A.2 中规定的 XCBC-MAC-96 模式下的 X。

9.5.2 密钥确认标识生成

MacTag,密钥确认标识,等于 MAC-KC(K,MsgID,ID_S,ID_R,PK_S,PK_R),并且应使用 A.2 规定的 SM4-XCBC-MAC-96_K(MsgID ‖ ID_S ‖ ID_R ‖ PK_S ‖ PK_R)和密钥 K 来计算。

9.5.3 密钥确认标识验证

“状态”,如果 MacTag′=MAC-KC (K,MsgID,ID_S,ID_R,PK_S,PK_R),MAC-KC-VER (K,MsgID,IDS,IDR,PKS,PKR,MacTag′)的返回值为真。

9.6 数据加密

9.6.1 概述

使用 GM/T 0002—2012 中规定的数据加密算法。

数据加密模式应为 GB/T 17964—2008 的第 9 章“计数器(CTR)”模式中规定的 CTR 模式。

9.6.2 计数器的初始值(IV)

为了避免发送计数器的初始值,计数器的初始值由两个实体根据随机数计算产生。

计数器的初始值 IV 等于 MAC-IV (MK,KI,NonceS,NonceR),应使用 A.1 中规定的 SM4-XCBC-PRF-128MK (KI ‖ NonceS ‖ NonceR ‖ (04))和密钥 MK 来计算。

9.6.3 加密

应使用 GB/T 17964—2008 中 9.2 “加密”所规定的加密密钥 KE 来加密数据:

$$EncData = ENC_{KE}(Data)$$

由于是 CTR 模式,不应使用填充数据。

9.6.4 解密

应使用 GB/T 17964—2008 中 9.3 “解密”所规定的加密密钥 KE 来解密加密数据。

$$Data' = DEC_{KE}(EncData)$$

9.7 数据完整性

9.7.1 概述

SCH 上传输的所有数据完整性应通过一个 MAC 保护。

用于数据完整性的 MAC 应为 A.2 中规定的 SM4-XCBC-MAC-96 模式下的 X 算法。

9.7.2 保护数据完整性

消息鉴别码 MAC 等于 MAC-DI(KI,SN,DataLen,EncData),而且应用 A.2 中规定的 SM4-XCBC-MAC-96KI (SN ‖ DataLen ‖ EncData) 和密钥 KI 来计算。

9.7.3 检查数据完整性

“状态”,如果 Mac′=MAC-DI (KI,SN ‖ DataLen ‖ EncData),MAC-DI-VER (KI,SN,DataLen,EncData,Mac′)的返回值为真。

9.8 信息序列完整性

信息序列完整性应根据 GB/T 33746.1—2017 中 12.3 的规定来处理。

SNV 值应在 0 到 $2^{24}-1$ 范围内，初始值为 0。

当 SNV 等于 $2^{24}-1$ 时，实体应终止 SCH。

10 数据转换

10.1 整数到字节串的转换

整数到字符串的转换应符合 GM/T 0003—2012 的规定。

10.2 字节串到整数的转换

字符串到整数的转换应符合 GM/T 0003—2012 的规定。

10.3 点到字节串的转换

点到字符串的转换应符合 GM/T 0003—2012 的规定。

10.4 字节串到点的转换

字符串到点的转换应符合 GM/T 0003—2012 的规定。

11 SSE 和 SCH 服务调用

11.1 概述

SSE 和 SCH 服务是通过建立两个 NFC-SEC 实体之间共享秘密来调用的，共享秘密通过 GB/T 33746.1 中定义的密钥协商和密钥确认协议来建立。本章将进一步明确图 1 中描述的这个过程。

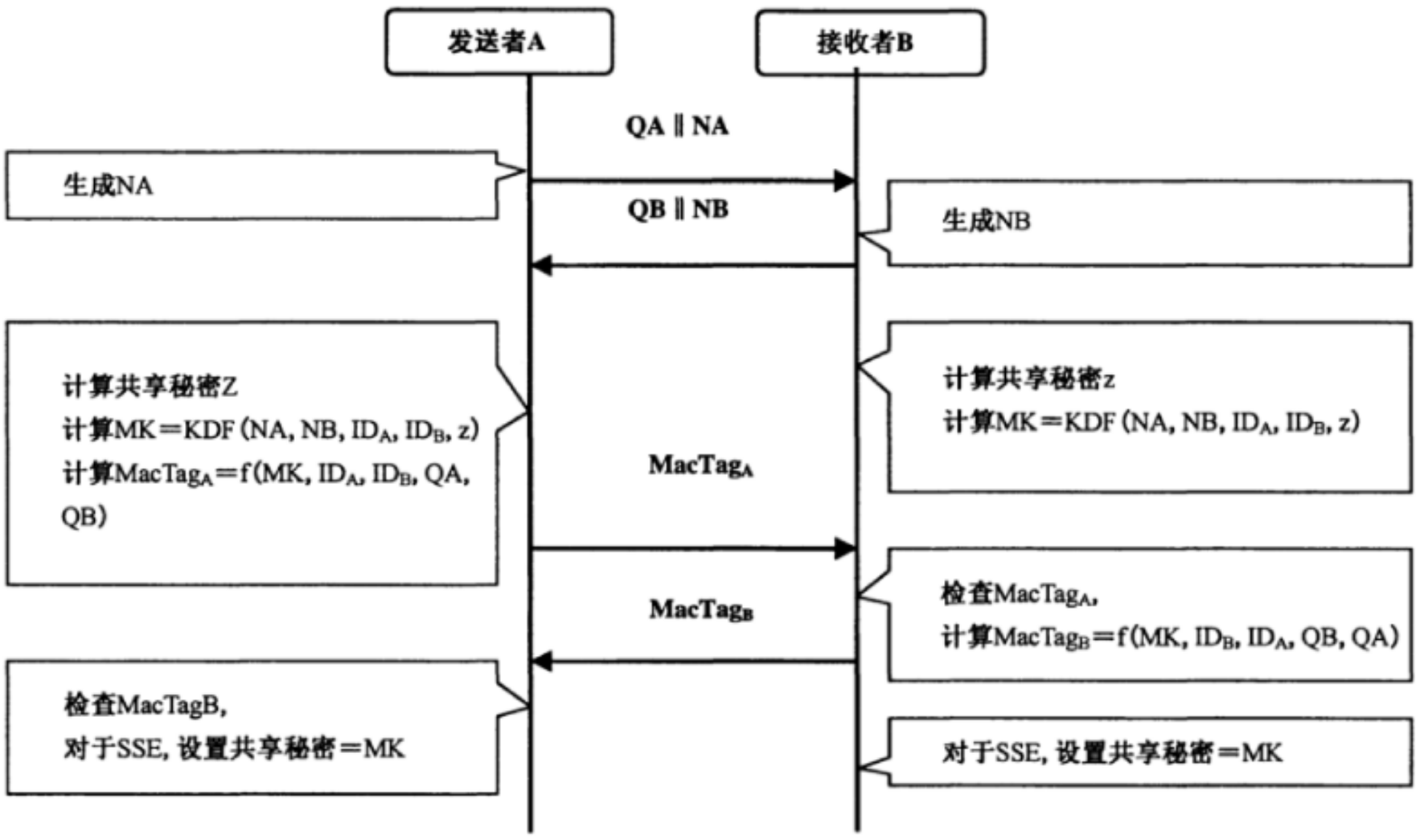

图 1 密钥协定和密钥确认概述

11.2 前提条件

在开始服务前，对于每个 NFC-SEC 实体以下部分需要提供：

根据 9.2.3 规定生成自身的公钥和私钥以及用于密钥交换的临时密钥对。

注：何时(以及以什么频率)生成密钥对，以及密钥交换双方的公钥或公钥证书等信息何时交换，已超出了本部分的范围。

ISO/IEC 18092:2004 中规定的它自身的 nfcid3 和其他的 NFC-SEC 实体的 nfcid3。

11.3 密钥协商

11.3.1 概述

密钥协商的过程见表 3。

表 3 密钥协商过程

发送者(A)	PDU 传输 (通信方向由箭头表示，有效载荷显示在括号中)	接收者(B)
生成随机数 NA		
压缩 Q_A		
发送给 B	A→B: ACT_REQ (QA ‖ NA)	
		生成随机数 NB
		压缩 Q_B
	A←B: ACT_RES (QB ‖ NB)	发送给 A
从 QB′重建 Q_B'		从 QA′重建 Q_A'
检查 Q_B'		检查 Q_A'
计算共享秘密:Z		计算共享秘密:Z

11.3.2 发送者(A)转换

转换步骤如下：

a) 根据 9.2.6 生成随机数 NA；

b) 根据 10.3 确定 QA 为字节串 QA；

c) 发送 QA ‖ NA 作为 ACT_REQ PDU 的有效载荷；

d) 从 ACT_RES PDU 的有效载荷中接收 QB′ ‖ NB′；

e) 根据 10.4 由 QB′重建 Q_B'；

如果已经收到公钥，先前计算和存储的 QB′值可重用，则下面的步骤可跳过；

f) 根据 9.2.4 验证是否 QB′是有效密钥。如果是无效的，则在协议机设置“PDU 内容有效”为假，跳过步骤 g)和 h)；

g) 根据 9.2.5 进行密钥推导。如果输出 z 是“无效的”，则在协议机设置“PDU 内容有效”为假，跳过步骤 h)；

h) 根据 10.1 中的规定转化 z 为字节串 Z。

11.3.3 接收者(B)转换

转换步骤如下：

a) 从 ACT_REQ PDU 有效载荷中接收 $QA' \| NA'$；

b) 根据 9.2.6 生成随机数 NB；

c) 根据 10.3 确定 QB 为字节串 QB；

d) 发送 $QB \| NB$ 作为 ACT_RES PDU 的有效载荷；

e) 根据 10.4 由 QA'重建 Q_A'；
如果已经得到公钥，先前计算存储的 Q_A'值可重用，且下面的步骤可跳过；

f) 根据 9.2.4 验证是否 QA'是有效密钥。如果是无效的，在协议机设置“PDU 内容有效”为假，步骤 g)和 h)可以省略；

g) 使用 9.2.5 进行密钥推导。如果输出 z 是“无效的”，则在协议机设置“PDU 内容有效”为假，跳过步骤 h)；

h) 根据 10.1 转化 z 为字节串 Z。

11.4 密钥导出

11.4.1 发送者(A)转换

对于 SSE 服务，根据 9.3.2 得到：MK_{SSE} = KDF-SSE (NA, NB′, Z, ID_A, ID_B)。

对于 SCH 服务，根据 9.3.4 得到：{MK_{SCH}, KE_{SCH}, KI_{SCH}} = KDF-SCH (NA, NB′, Z, ID_A, ID_B)。

11.4.2 接收者(B)转换

对于 SSE 服务，根据 9.3.2 得到：MK_{SSE} = KDF-SSE (NA′, NB, Z, ID_A, ID_B)。

对于 SCH 服务，根据 9.3.3 得到：{MK_{SCH}, KE_{SCH}, KI_{SCH}} = KDF-SCH (NA′, NB, Z, ID_A, ID_B)。

11.5 密钥确认

11.5.1 概述

密钥确认的过程见表 4。

表 4 密钥确认的过程

发送者(A)	PDU 传输 (通信方向由箭头表示，有效载荷显示在括号中)	接收者(B)
计算密钥确认标识：$MacTag_A$(MK)		
发送到 B	A→B： VFY_REQ($MacTag_A$)	
		检查从 A 接收的密钥确认标识：$MacTag_A'$(MK)
		计算密钥确认标识：$MacTag_B$(MK)
	A←B： VFY_RES ($MacTag_B$)	
检查从 B 接收的密钥确认标识：$MacTag_B'$(MK)		
对于 SSE，设置共享秘密值为 MK		对于 SSE，设置共享秘密值为 MK

11.5.2 发送者(A)转换

转换步骤如下：

a) 根据 9.5.2，计算从 A 到 B 的密钥确认标识，MacTagA＝MAC-KC(MK,(03),IDA,IDB,QA,QB′)；

b) 发送 MacTagA 作为 VFY_REQ PDU 的有效载荷；

c) 从 VFY_RES PDU 的有效载荷接收 MacTagB′；

d) 检查从 B 到 A 的密钥确认标识。根据 9.5.3 在协议机设置 MAC-KC-VER(MK,(02),IDB,IDA,QB′,QA,MacTagB′)的输出为“PDU 内容有效”。如果无效，跳过步骤 e)；

e) 对于 SSE 服务，设置共享秘密＝ MKSSE 。

11.5.3 接收者(B)转换

转换步骤如下：

a) 从 VFY_REQ PDU 的有效载荷接收 MacTagA′；

b) 检查从 A 到 B 的密钥确认标识。根据 9.5.3 在协议机设置 MAC-KC-VER (MK,(03),IDA,IDB,QA′,QB,MacTagA′)的输出为“PDU 内容有效”。如果无效，跳过步骤 c),d)和 e)；

c) 根据 9.5.2 计算从 B 到 A 密钥确认标识 MacTagB＝MAC-KC(MK ,(02),IDB,IDA,QB,QA′)；

d) 发送 MacTagB 作为 VFY_RES PDU 的有效载荷；

e) 对于 SSE 服务，设置共享秘密＝MKSSE。

12 SCH 数据交换

12.1 概述

根据第 11 章中的定义，SCH 调用后，两个 NFC-SEC 实体间的数据交换根据 GB/T 33746.1—2017 中的规定来进行，如图 2 所示，本章中将进一步明确。

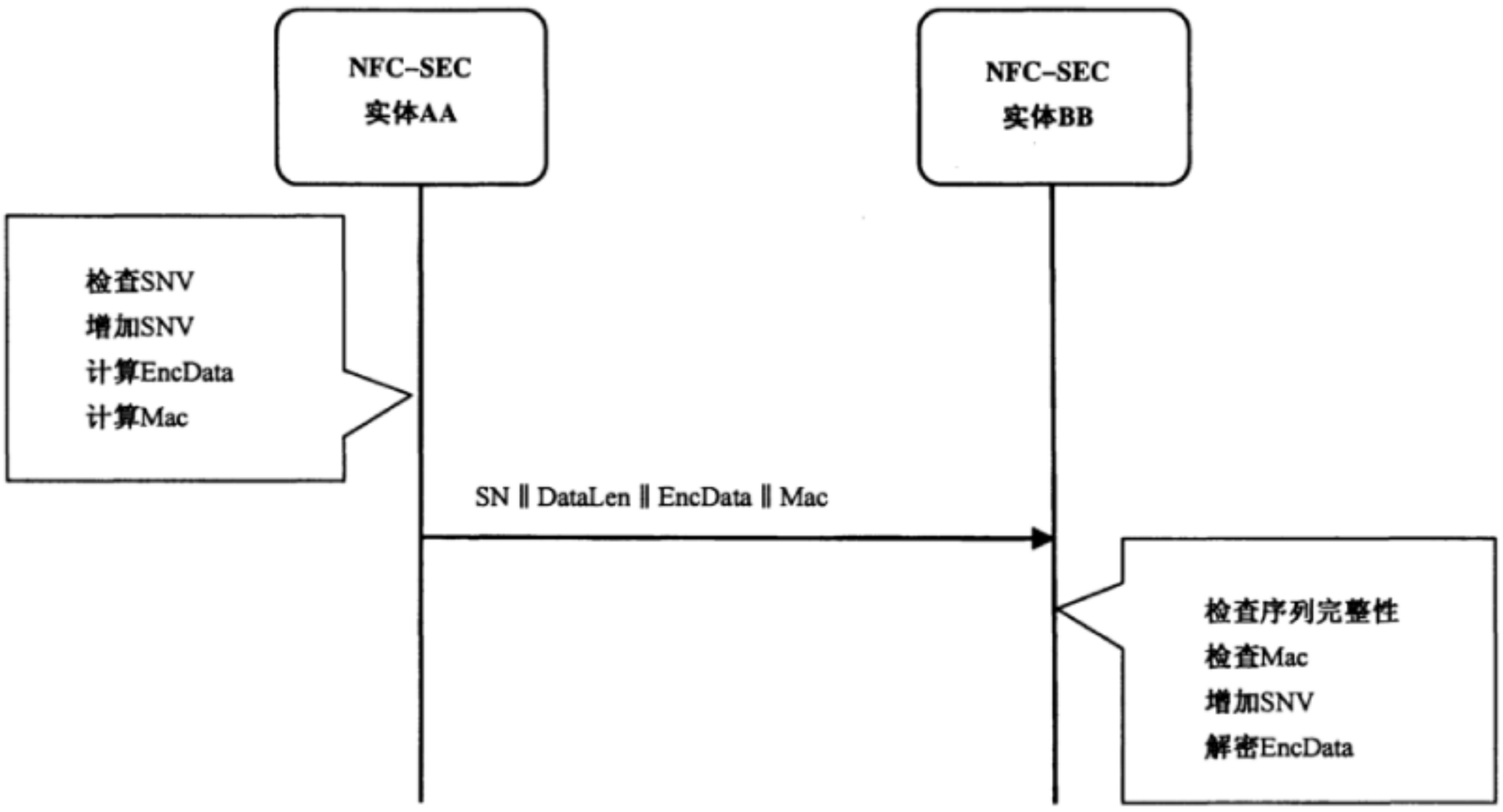

图 2 SCH 协议概述

12.2 准备

NFC-SEC 实体(AA 和 BB)应执行以下准备步骤：

a) 根据 9.6.2 生成 CTR 计数器初值,IV＝MAC-IV (MK,KI,NAA,NBB)；

b) 根据 9.8 初始化序列号变量 SNV。

12.3 数据交换

12.3.1 数据交换概述

数据交换的过程见表 5。

表 5 数据交换的过程

发送对等实体 AA **(A 或 B)**	PDU 传输 (通信方向由箭头表示,有效载荷显示在括号中)	**接收对等实体 BB** **(B 或 A)**
• 从发送数据 SDU 接收 UserData • 检查 SNV • 增加 SNV • 加密数据:EncData • 使用 MAC:Mac		
	ENC (SNV ‖ DataLen ‖ EncData ‖ Mac)	
		接收： • 检查序列完整性 • 检查数据完整性 • 增加 SNV • 解密数据

12.3.2 发送

发送数据时,发送的 NFC-SEC 对等实体 AA(A 或 B)应执行以下步骤：

a) 从发送数据 SDU 接收 Userdata；

b) 如果 SNV＝$2^{24}-1$,则在协议机中设置“PDU 内容有效”为假,否则执行下列步骤；

c) 根据 GB/T 33746.1—2017 中 12.3 的规定增加 SNV；

d) 根据 9.6.3 从 Userdata 计算出加密数据 EncData；

e) 通过 SNV ‖ DateLen ‖ EncData,根据 9.7.2 中的方法计算 MACMac；

f) 发送 SNV ‖ DataLen ‖ EncData ‖ Mac 作为 ENC PDU 的有效载荷。

12.3.3 接收

接收数据时,接收的 NFC-SEC 对等实体 BB(B 或 A)应执行以下步骤：

a) 从 ENC PDU 的有效载荷中接收 SNV ‖ DataLen ‖ EncData ‖ Mac；

b) 如果 SNV＝$2^{24}-1$,则在协议机中设置“PDU 内容有效”为假,否则执行下列步骤；

c) 根据 GB/T 33746.1—2017 中 12.3 检查序列完整性；

d) 根据 GB/T 33746.1—2017 中 12.3 的规定增加 SNV；

e) 根据 9.7.3 检查 SNV ‖ DataLen ‖ EncData 数据完整性。如果是无效的，则在协议机中设置“PDU 内容有效”为假，否则执行下列步骤；

f) 根据 9.6.4 从 EncData 计算解密数据 UserData。

附 录 A
（规范性附录）
SM4-XCBC-PRF-128 和 SM4-XCBC-MAC-96 算法

A.1 SM4-XCBC-PRF-128

SM4-XCBC-PRF-128 算法是一个带有强制“10 * 序列填充”的基本 CBC-MAC 的变体，可保障任意长度信息安全。

加密操作应使用一个 128 位密钥的 SM4 算法完成。本部分采用的 SM4 算法应符合国家对密码管理的相关规定。

给定 128 位密钥 K，SM4-XCBC-PRF-128 按以下方式计算，信息 M 由 n 块组成 M[1] ... M[n]，M[1] ... M[$n-1$]块长度均为 128 比特，M[n]块长度在 1～128 比特之间：

a) 按以下公式从 128 比特密钥 K 生成 3 个 128 比特密钥(K1，K2 和 K3)：
K1＝(01010101010101010101010101010101) 用密钥 K 加密；
K2＝(02020202020202020202020202020202) 用密钥 K 加密；
K3＝(03030303030303030303030303030303) 用密钥 K 加密。

b) 定义 E[0]＝0x00000000000000000000000000000000。

c) 对于每一个块 M[i]，当 i＝1...$n-1$ 时：
M[i] XOR E[$i-1$]，之后把结果用密钥 K1 加密，产生 E[i]。

d) 对于块 M[n]：

1) 如果 M[n]的块大小是 128 比特：
M[n] XOR E[$n-1$] XOR 密钥 K2，
之后把结果用密钥 K1 加密，产生 E[n]。

2) 如果 M[n]块的大小小于 128 比特：

i) M[n]不足的部分交替填充比特“1”之后是比特“0”(可能无)直到 M[n]块补齐到 128 位(这就是“10 * 序列填充”)。

ii) M[n]XOR E[$n-1$] XOR 密钥 K3，之后把结果用密钥 K1 加密，产生 E[n]。

e) 输出结果是最后的 128 位块 E[n]。

A.2 SM4-XCBC-MAC-96

SM4-XCBC-MAC-96 算法就是首先运行 SM4-XCBC-PRF-128 算法，之后跟随以下截取步骤：
截取 E[n]前 96 比特位
发送时，截取值存储在鉴别者字段(Mac)中。
接收时，计算整个 128 位比特值，前 96 比特与存储在鉴别者字段(Mac)的值进行比较。

附 录 B
（规范性附录）
字段长度

字段长度见表 B.1。

表 B.1 字段长度

字段	长度
NA	96 比特
NB	96 比特
d_A	256 比特
d_B	256 比特
D_A	256 比特
D_B	256 比特
DataLen	24 比特
Q_A	512 比特
Q_B	512 比特
QA	264 比特
QB	264 比特
Z	256 比特
MK	128 比特
KE	128 比特
KI	128 比特
$MacTag_A$	96 比特
$MacTag_B$	96 比特
IV	128 比特
SNV	24 比特
Mac	96 比特

附 录 C
（规范性附录）
NEAU-A 鉴别机制

C.1 NEAU-A 鉴别机制概述

本附录规定了 NFC 实体鉴别机制 NEAU-A，该机制采用了 ISO/IEC 9798-3:1998/Amd.1:2010 中的 TePA 实体鉴别技术和 GB/T 28455—2012 中的 TePA-AC 技术。NEAU-A 的鉴别过程如图 C.1 所示，在需要时可信第三方将参与鉴别过程，为发送者 A 和接收者 B 提供鉴别服务，对第三方 TTP 的支持为机制必备能力。同时，本机制能够基于 ISO/IEC 20009-2:2013 规定的匿名鉴别机制支持发送者 A 和接收者 B 的匿名需求。

本附录涉及的密码算法应符合国家对密码管理的相关规定。

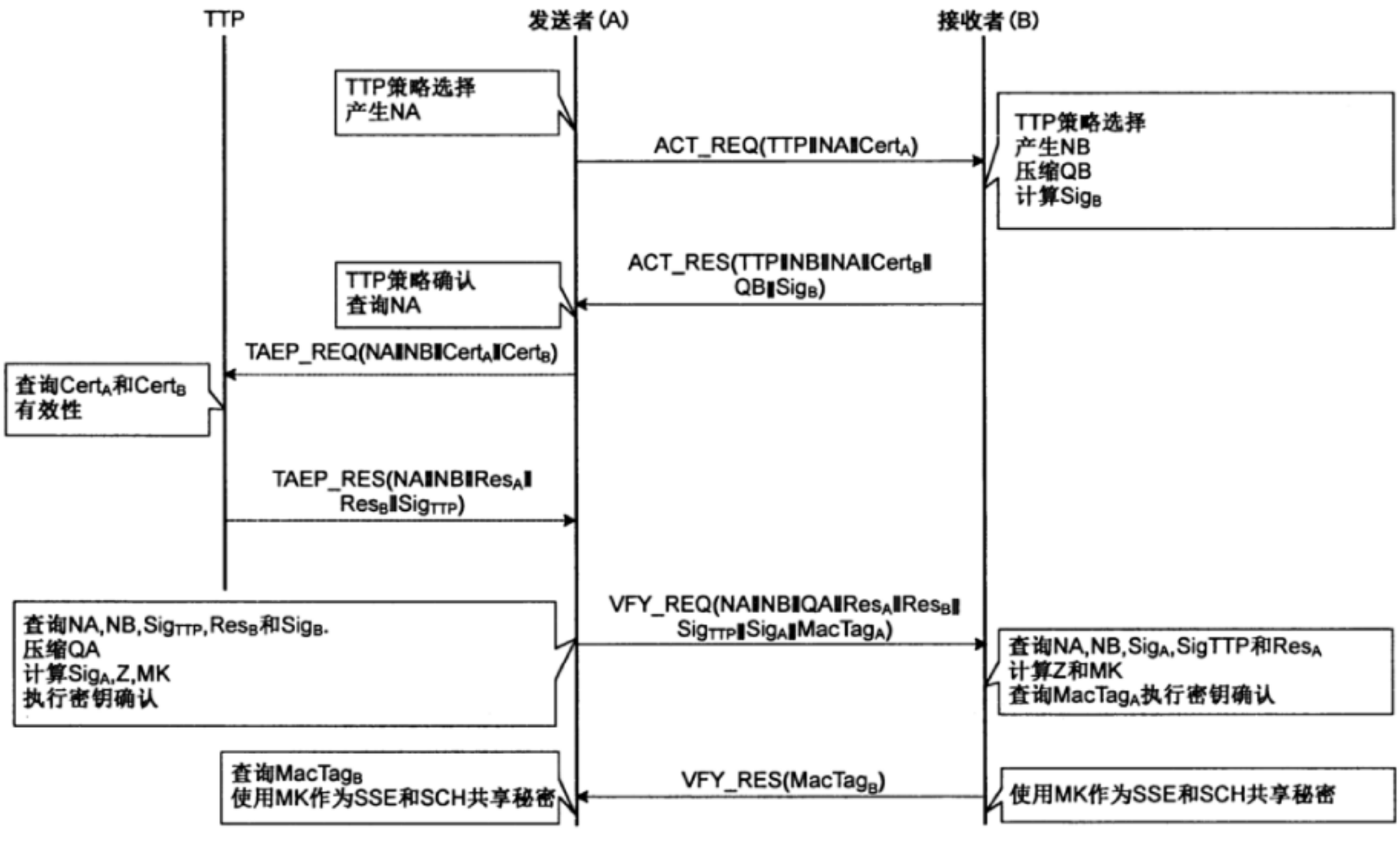

图 C.1 NEAU-A 实体鉴别协议概述

C.2 准备

在开始服务前，对于每个 NFC-SEC 实体需具备以下部分：

——各自具备数字证书 $Cert_A$、$Cert_B$、$Cert_{TTP}$和对应的私钥。

——在支持可信第三方调用的情况下，实体 A 和实体 B 具备 TTP 的数字证书 $Cert_{TTP}$。

——ISO/IEC 18092:2004 中规定的它自身的 nfcid3 和其他 NFC-SEC 实体的 nfcid3。

——每个 NFC-SEC 实体知道自己是否支持 TTP 的策略，发送方知道是否 TTP 是可以连接的。

C.3 支持可信第三方 TTP 的鉴别流程

C.3.1 实体 A 向实体 B 发送包括 TTP ‖ NA ‖ $Cert_A$ 的 ACT_REQ 鉴别消息，其中，NA 为实体 A 产生的随机数，$Cert_A$ 为实体 A 的证书，TTP 代表是否引入参与鉴别过程。

C.3.2 实体 B 收到来自实体 A 的 ACT_REQ 鉴别消息后，如果身份鉴别方式支持第三方，则实体 B 产生随机数 NB，利用自身的私钥 CS_B 计算数字签名 $Sig_B = SIG(CS_B, ID_A \| ID_B \| TTP \| NA \| NB \| QB)$，其中 SIG 为 SM2 数字签名算法，$ID_A$ 和 ID_B 分别为实体 A 和实体 B 的标识信息，QB 为实体 B 的临时公钥，实体 B 向实体 A 发送包括 TTP ‖ NB ‖ NA ‖ $Cert_B$ ‖ QB ‖ Sig_B 的 ACT_RES 鉴别消息，其中 $Cert_B$ 为实体 B 的证书。

C.3.3 实体 A 收到来自实体 B 的 ACT_RES 鉴别消息后，如果身份鉴别方式支持第三方，则实体 A 向实体 TTP 发送包括 NA ‖ NB ‖ $Cert_A$ ‖ $Cert_B$ 的 TAEP_REQ 鉴别消息。

C.3.4 实体 TTP 收到来自实体 A 的包括 NA ‖ NB ‖ $Cert_A$ ‖ $Cert_B$ 的 TAEP_REQ 鉴别消息后，根据 $Cert_A$ 和 $Cert_B$ 的有效性对实体 A 和实体 B 的合法性进行鉴别，根据鉴别结果组成 Res_A 和 Res_B，其中 Res_A 和 Res 分别包含对实体 A 和实体 B 的鉴别结果和对应的证书；利用自身的私钥 CS_{TTP} 计算数字签名 $Sig_{TTP} = SIG(CS_{TTP}, NA \| NB \| Res_A \| Res_B)$，其中 SIG 为 SM2 数字签名算法，实体 TTP 向实体 A 发送包括 NA ‖ NB ‖ Res_A ‖ Res_B ‖ Sig_{TTP} 的 TAEP_RES 鉴别消息。

C.3.5 实体 A 收到来自实体 TTP 的 TAEP_RES 鉴别消息后，进行验证：

a) 验证 TAEP_RES 鉴别消息中 Sig_{TTP} 中实体 TTP 的签名，并检查 TAEP_REQ 鉴别消息中实体 A 产生的随机数 NA 与包含在 Sig_{TTP} 中实体 TTP 的签名数据中的随机数 NA 是否相符，若验证通过则执行 b)；

b) 得到实体 B 的验证结果 Res_B，若实体 B 合法有效，则执行 c)，否则实体 A 完成对实体 B 的鉴别，则实行 C.3.6；

c) 获得实体 B 的公钥，验证 ACT_RES 鉴别消息中 Sig_B 的数字签名，并检查实体 A 的标识信息 ID_A 与包含在 Sig_B 签名数据中的标识信息 ID_A 是否一致，校验 ACT_REQ 鉴别消息中的随机数 NA 与包含在 Sig_B 签名数据中的随机数 NA 是否一致，若验证通过，实体 A 完成对实体 B 的鉴别，则实行 C.3.7。

C.3.6 实体 A 利用自身的私钥 CS_A 计算实体 A 的数字签名 $Sig_A = SIG(CS_A, ID_A \| ID_B \| NA \| NB \| QA)$，其中 QA 为实体 A 的临时公钥；实体 A 检查是否已存储有实体 B 的临时公钥 QB，若已存储有 QB，则使用已存储的 QB，否则检查收到的 ACT_RES 鉴别消息中的 QB 的有效性，如果有效，则使用收到的 ACT_RES 鉴别消息中的 QB，如果无效，则终止鉴别；体 A 基于 SM2 密钥交换协议，利用实体 A 事先产生的临时私钥 d_A 和实体 B 的临时公钥 QB 计算秘密信息 $z = f(d_A, QB)$，其中 f 指 SM2 密钥交换协议的密钥计算函数，如果计算出错，则终止鉴别，否则，实体 A 将计算出的秘密信息 z 转换为字符串 Z，计算密钥 MK = KDF(NA, NB, Z, ID_A, ID_B)，其中 KDF 指 9.3 密钥推导算法，计算消息鉴别码 $MacTag_A = MAC(MK, ID_A, ID_B, QA, QB)$，其中 MAC 为 9.5 消息鉴别码计算方法，并发送包括 NA ‖ NB ‖ QA ‖ Res_A ‖ Res_B ‖ Sig_{TTP} ‖ Sig_A ‖ $MacTag_A$ 的 VFY_REQ 鉴别消息给实体 B。

C.3.7 实体 B 接收到来自实体 A 的 VFY_RES 鉴别消息后，检查 VFY_RES 鉴别消息中字段数据的正确性：

a) 验证 VFY_RES 鉴别消息中 Sig_{TTP} 中实体 TTP 的签名，并检查 TAEP_RES 鉴别消息中实体 B 产生的随机数 NB 与包含在 Sig_{TTP} 中实体 TTP 的签名数据中的随机数 NB 是否相符，若验证通过则执行 b)；

b) 得到实体 A 的验证结果 Res_A，若实体 A 合法有效，则执行 c)，否则实体 A 完成对实体 B 的鉴别，则终止鉴别过程；

c) 获得实体 A 的公钥，验证 VFY_RES 鉴别消息中 Sig_A 的数字签名，并检查实体 B 的标识信息

ID_B 与包含在 Sig_A 签名数据中的标识信息 ID_B 是否一致，校验 ACT_REQ 鉴别消息中的随机数 NB 与包含在 Sig_A 签名数据中的随机数 NB 是否一致，若验证通过，实体 B 完成对实体 A 的鉴别，则实行 C.3.8。

C.3.8 实体 B 检查是否已存储有实体 A 的临时公钥 QA，若已存储有 QA，则使用已存储的 QA，否则检查收到的 VFY_RES 鉴别消息中的 QA 的有效性，如果有效，则使用收到的 VFY_REQ 鉴别消息中的 QA，如果无效，则终止鉴别。

C.3.9 实体 B 基于 SM2 密钥交换协议，利用实体 B 事先产生的临时私钥 d_B 和实体 A 的临时公钥 QA 计算秘密信息 $z=f(d_B,QA)$，如果计算出错，则终止鉴别，否则，实体 B 将计算出的秘密信息 z 转换为字符串 Z，并计算密钥 MK= KDF(NA,NB,Z,ID_A,ID_B)，计算消息鉴别码 $MacTag_A$=MAC(MK,ID_A,ID_B,QA,QB)，并与收到的实体 A 发送的 VFY_RES 鉴别消息中的 $MacTag_A$ 进行比较，如果不相等，则密钥确认失败，终止鉴别过程；否则，计算消息鉴别码 $MacTag_B$=MAC(MK,IDB,IDA,QB,QA)，将包括 $MacTag_B$ 的 VFY_RES 鉴别消息发送给实体 A。

C.3.10 实体 A 收到来自实体 B 的 VFY_RES 鉴别消息后，计算 $MacTag_B$=MAC(MK,IDB,IDA,QB,QA)，并与收到的 VFY_RES 鉴别消息中的 $MacTag_B$ 进行比较，如果不相等，则密钥确认失败；如果相等，则认为密钥确认成功。

C.4 不支持可信第三方 TTP 的鉴别流程

C.4.1 实体 A 向实体 B 发送包括 TTP ‖ NA ‖ $Cert_A$ 的 ACT_REQ 鉴别消息，其中，NA 为实体 A 产生的随机数，$Cert_A$ 为实体 A 的证书，TTP 代表是否引入参与鉴别过程。

C.4.2 实体 B 收到来自实体 A 的 ACT_REQ 鉴别消息后，如果身份鉴别方式不支持第三方，则检查证书 $Cert_A$ 的有效性，若证书无效，则终止鉴别。

C.4.3 实体 B 产生随机数 NB，利用自身的私钥 CS_B 计算数字签名 Sig_B=SIG(CS_B,ID_A ‖ ID_B ‖ TTP ‖ NA ‖ NB ‖ QB)，其中 SIG 为 SM2 数字签名算法，ID_A 和 ID_B 分别为实体 A 和实体 B 的标识信息，QB 为实体 B 的临时公钥，实体 B 向实体 A 发送包括 TTP ‖ NB ‖ NA ‖ $Cert_B$ ‖ QB ‖ Sig_B 的 ACT_RES 鉴别消息，其中 $Cert_B$ 为实体 B 的证书。

C.4.4 实体 A 收到来自实体 B 的 ACT_RES 鉴别消息后，如果身份鉴别方式不支持第三方，则检查 ACT_RES 鉴别消息中字段数据的正确性，若验证不正确，则终止鉴别。

C.4.5 实体 A 利用自身的私钥 CS_A 计算实体 A 的数字签名 Sig_A=SIG(CS_A,ID_A ‖ ID_B ‖ NA ‖ NB ‖ QA)，其中 QA 为实体 A 的临时公钥；实体 A 检查是否已存储有实体 B 的临时公钥 QB，若已存储有 QB，则使用已存储的 QB，否则检查收到的 ACT_RES 鉴别消息中的 QB 的有效性，如果有效，则使用收到的 ACT_RES 鉴别消息中的 QB，如果无效，则终止鉴别。

C.4.6 实体 A 基于 SM2 密钥交换协议，利用实体 A 事先产生的临时私钥 d_A 和实体 B 的临时公钥 QB 计算秘密信息 $z=f(d_A,QB)$，其中 f 指 SM2 密钥交换协议的密钥计算函数，如果计算出错，则终止鉴别，否则，实体 A 将计算出的秘密信息 z 转换为字符串 Z，计算密钥 MK= KDF(NA,NB,Z,ID_A,ID_B)，其中 KDF 指 9.3 密钥推导算法，计算消息鉴别码 $MacTag_A$=MAC(MK,ID_A,ID_B,QA,QB)，其中 MAC 为 9.5 消息鉴别码计算方法，并发送包括 NA ‖ NB ‖ QA ‖ Sig_A ‖ $MacTag_A$ 的 VFY_REQ 鉴别消息给实体 B。

C.4.7 实体 B 接收到来自实体 A 的包括 NA ‖ NB ‖ QA ‖ Sig_A ‖ $MacTag_A$ 的 VFY_RES 鉴别消息后，检查第 VFY_RES 鉴别消息中字段数据的正确性，若验证不正确，则终止鉴别。

C.4.8 实体 B 检查是否已存储有实体 A 的临时公钥 QA，若已存储有 QA，则使用已存储的 QA，否则检查收到的 VFY_RES 鉴别消息中的 QA 的有效性，如果有效，则使用收到的 VFY_REQ 鉴别消息中的 QA，如果无效，则终止鉴别。

C.4.9 实体 B 基于 SM2 密钥交换协议，利用实体 B 事先产生的临时私钥 d_B 和实体 A 的临时公钥 QA

计算秘密信息 $z=f(d_B,QA)$，如果计算出错，则终止鉴别，否则，实体 B 将计算出的秘密信息 z 转换为字符串 Z，并计算密钥 $MK=KDF(NA,NB,Z,ID_A,ID_B)$，计算消息鉴别码 $MacTag_A=MAC(MK,ID_A,ID_B,QA,QB)$，并与收到的实体 A 发送的 VFY_REQ 鉴别消息中的 $MacTag_A$ 进行比较，如果不相等，则终止鉴别；否则，实体 B 认为实体 A 合法，并计算消息鉴别码 $MacTag_B=MAC(MK,IDB,IDA,QB,QA)$，将包括 $MacTag_B$ 的 VFY_RES 鉴别消息发送给实体 A。

C.4.10 实体 A 收到来自实体 B 的 VFY_RES 鉴别消息后，计算 $MacTag_B=MAC(MK,IDB,IDA,QB,QA)$，并与收到的 VFY_RES 鉴别消息中的 $MacTag_B$ 进行比较，如果不相等，则认为实体 B 非法；如果相等，则认为实体 B 合法。

C.5 密钥推导

C.5.1 发送者(A)

为 SSE 计算 $MK_{SSE}=KDF\text{-}SSE(NA,NB,Z,ID_A,ID_B)$。

为 SCH 计算 $\{MK_{SCH},KE_{SCH},KI_{SCH}\}=KDF\text{-}SCH(NA,NB,Z,ID_A,ID_B)$。

C.5.2 接收者(B)

为 SSE 计算 $MK_{SSE}=KDF\text{-}SSE(NA,NB,Z,ID_A,ID_B)$。

为 SCH 计算 $\{MK_{SCH},KE_{SCH},KI_{SCH}\}=KDF\text{-}SCH(NA,NB,Z,ID_A,ID_B)$。

附 录 D
（规范性附录）
NEAU-S 鉴别机制

D.1 NEAU-S 鉴别机制概述

NFC 实体鉴别机制 NEAU-S 基于两个 NFC-SEC 实体之间预共享的密钥来完成鉴别，过程如图 D.1 所示。

本附录涉及的密码算法应符合国家对密码管理的相关规定。

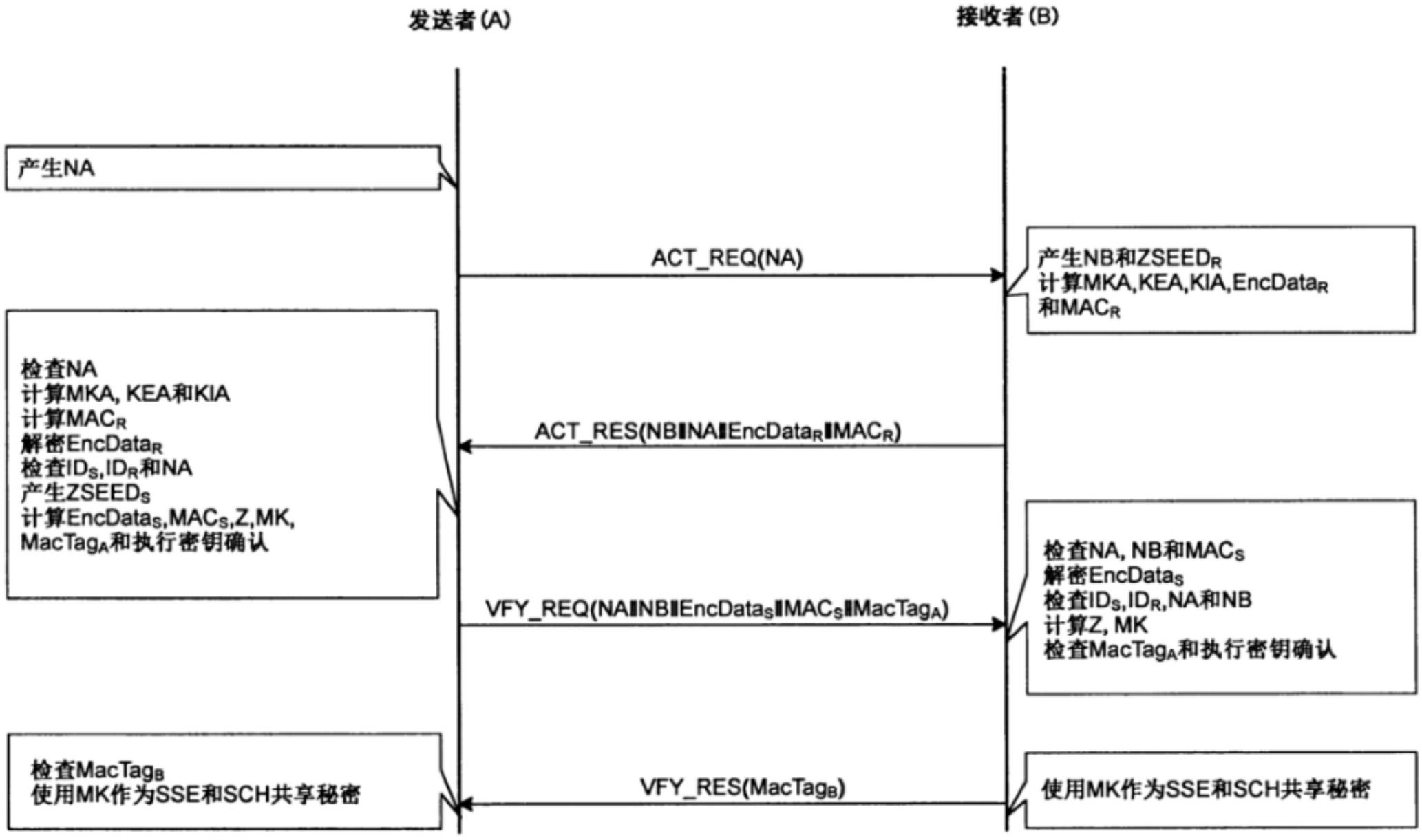

图 D.1 NEAU-S 实体鉴别概述

D.2 准备

在开始服务前，对于每个 NFC-SEC 实体应具备以下部分：

——各自具备预共享的鉴别密钥 MK；

——ISO/IEC 18092:2004 中规定的它自身的 nfcid3 和其他的 NFC-SEC 实体的 nfcid3。

D.3 流程

D.3.1 实体 A 产生随机数 NA，并发送给实体 B。

D.3.2 实体 B 收到 NA 后，生成随机数 NB 和用于作为密钥种子的随机数 $ZSEED_B$，计算密钥 MKA ‖ KEA ‖ KIA=KDF(NA,NB,PSK,ID_A,ID_B)，计算密文 $EncData_B$=Enc(KEA,NB ‖ NA ‖ IDB ‖ IDA ‖ $ZSEED_B$)，计算消息鉴别码 MAC_B=MAC(KIA,NB ‖ NA ‖ $EncData_B$)，实体 B 发送 NB ‖ NA ‖ Enc-

$Data_B \| MAC_B$ 给实体 A，其中，MKA 为鉴别密钥，KEA 为消息加密密钥，KIA 为消息完整性密钥，KDF 为 9.3 密钥推导算法，ID_A 为实体 A 的身份标识，ID_B 为实体 B 的身份标识，Enc 为加密算法，MAC 为 9.5 消息鉴别码计算方法。

D.3.3 实体 A 收到 $NB \| NA \| EncData_B \| MAC_B$ 后进行验证，若验证不正确，则终止鉴别。

D.3.4 实体 A 产生用于作为密钥种子的随机数 $ZSEED_A$，计算密文 $EncData_A = Enc(KEA, NA \| NB \| ID_A \| ID_B \| ZSEED_A)$，计算消息鉴别码 $MAC_A = MAC(KIA, NA \| NB \| EncData_A)$，计算共享秘密 $Z = ZSEED_A \oplus ZSEED_B$，计算主密钥 $MK = KDF(NA, NB, Z, ID_A, ID_B)$，计算消息鉴别标识 $MacTag_A = MAC(MK, MsgID1 \| ID_A \| ID_B \| NA \| NB)$，发送 $NA \| NB \| EncData_A \| MAC_A \| MacTag_A$ 给实体 B，其中，KDF 为 9.3 密钥推导算法，MsgID1 为一消息序列号，“⊕”表示逐比特异或，MAC 为 9.5 消息鉴别码生成算法。

D.3.5 实体 B 收到 $NA \| NB \| EncData_A \| MAC_A \| MacTag_A$ 后进行验证，若验证不正确，则终止鉴别。

D.3.6 实体 B 计算共享秘密 $Z = ZSEED_A \oplus ZSEED_B$，计算主密钥 $MK = KDF(NA, NB, Z, ID_A, ID_B)$，计算消息鉴别标识 $MacTag_A = MAC(MK, MsgID1 \| ID_A \| ID_B \| NA \| NB)$，并与收到的 $MacTag_A$ 进行比较，如果相等，则认为实体 A 身份合法；如果不相等，终止鉴别；其中，KDF 为 9.3 密钥推导算法。

D.3.7 实体 B 计算消息鉴别标识 $MacTag_B = MAC2(MK, MsgID2 \| ID_B \| ID_A \| NB \| NA)$，并将 $MacTag_B$ 发送给实体 A，其中，MsgID2 为一消息序列号。

D.3.8 实体 A 收到 $MacTag_B$ 后，首先计算消息鉴别标识 $MacTag_B = MAC2(MK, MsgID2 \| ID_B \| ID_A \| NB \| NA)$，然后将计算得到的 $MacTag_B$ 与收到的 $MacTag_B$ 进行比较，如果相等，则认为实体 B 身份合法。

中 华 人 民 共 和 国
国 家 标 准
近场通信(NFC)安全技术要求
第 2 部分:安全机制要求
GB/T 33746.2—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 45 千字
2017 年 9 月第一版 2017 年 9 月第一次印刷
*
书号:155066·1-55986 定价 27.00 元

GB/T 33746.2-2017