ICS 35.030
I65

团　体　标　准

T/SCCIA 013-2023

机器人通行领域的身份鉴别密码应用指南

Guidelines of Cryptographic Application for Identity Authentication in the Field of Robot Access

2023-7-18 发布　　2023-7-18 实施

深圳市商用密码行业协会　发布

目　　次

前言

本标准按照 GB/T 1.1-2020 给出的规则起草。

请注意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。

本标准由深圳市商用密码行业协会提出并归口。

本标准起草单位：深圳市旺龙智能科技有限公司，广东产品质量监督检验研究院，北京信长城科技发展有限公司，沃通电子认证服务有限公司，哈尔滨工业大学（深圳），鼎铉商用密码测评技术（深圳）有限公司，深圳市电子商务安全证书管理有限公司，深圳奥联信息安全技术有限公司，深圳市优必选科技股份有限公司，广州映博智能科技有限公司，深圳市智绘科技有限公司。

本标准主要起草人：李标彬、黄永康、丘彬、林彦霆、刘鹏、唐占国、何道敬、陈磊、杨振燕、但波、肖中胜、杨旭、郭巍、王胜男。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

机器人通行领域的身份鉴别密码应用指南

1 范围

本标准针对机器人及其身份生成系统、分发系统、出入口控制系统，提出了系统中使用的密码算法、密码设备、密码协议和密钥管理的相关建议。

本标准适用于指导采用机器人通行领域的身份鉴别的出入口控制系统相关产品的研制、使用和管理。

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 15843.2 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918.1 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 38635.1 信息安全技术 SM9标识密码算法 第1部分：总则

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GB/T 41389 信息安全技术 SM9密码算法使用规范

GM/T 0015 基于SM2密码算法的数字证书格式

GM/T 0034 基于SM2密码算法的证书认证系统密码及其相关安全技术规范

GM/T 0080 SM9密码算法使用规范

GM/T 0086 基于SM9标识密码算法的密钥管理系统技术规范

GM/Z 4001 密码术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

密钥分散 key distribution

为防止上级密钥泄露，利用上级密钥对其在本级使用的特征数据进行加密运算，得到适合在本级使用的密钥的过程。

3.2

根密钥 root key

系统最上层的密钥。

3.3

子密钥 sub key

利用根密钥分散得到的密钥。

3.4

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.5

身份唯一标识符 unique identifier

系统为机器人颁发的系统内唯一标识符，代表机器人身份的标识符。

3.6

机器人 robot

是一种能够半自主或全自主工作的智能移动机器。通常无法像人类一样开门通行或自行乘坐电梯等。

3.7

机器人通行领域的身份鉴别 identity verification in the field of robot access

指机器人在通行一些受管控的区域的出入口时，这些出入口的安全控制系统要对机器人身份的真伪进行实体鉴别的过程。

4 符号和缩略语

4.1 符号

下列符号适用于本文件。

Dec(K,X)：解密运算符，用密钥K对X进行解密运算

Enc(K,X)：加密运算符，用密钥K对X进行加密运算

HMAC(K,X)：采用哈希算法计算的消息认证码（Hash-based Message Authentication Code），用密钥K对X进行哈希计算得到的消息认证码

⊕：比特异或

4.2 缩略语

下列缩略语适用于本文件。

CA：证书授权（Certificate Authority）

CPU：中央处理器（Central Processing Unit）

IBC：基于标识的密码技术（Identity-Based Cryptograph）

PKI：公钥基础设施（Public Key Infrastructure）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

TLS：传输层安全性协议（Transport Layer Security）

UID：身份唯一标识符(Unique IDentifier)

UID_M：系统为机器人厂商颁发的系统内唯一的厂商标识（Unique IDentifier)

UID_R：机器人厂商为机器人颁发的厂商内唯一标识，和厂商标识一起，构成机器人的身份唯一标识符(Unique IDentifier)

5 密码应用系统概述

5.1 系统构成

基于机器人通行领域各类系统的密码应用涉及机器人及其身份生成系统、分发系统、出入口控制系统，如图 1 所示。各系统通过自身的密码模块提供所需的密码服务。

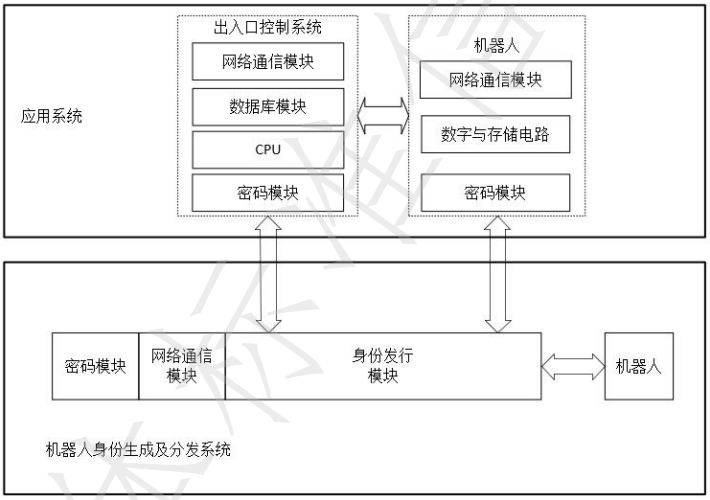

图 1 系统中密码应用结构图

5.1.1 机器人身份生成及分发系统

机器人身份生成及分发系统负责利用密码技术，给系统内所有机器人的唯一身份标识生成能鉴别其真实性的密钥或证书，并将该身份标识以及密钥或证书等信息安全分发给机器人以及出入口控制设备。相应密码模块提供匹配的密钥或证书存储、使用和管理能力。

5.1.2 出入口控制系统

出入口控制系统负责从身份生成及分发系统中安全导入机器人身份标识鉴别所需的密钥或证书，并利用密钥或证书对要通行的机器人身份进行鉴别，确定通行的机器人的身份的合法性。相应密码模块提供匹配的密钥或证书存储、使用和管理能力。

5.1.3 机器人

机器人负责从身份生成及分发系统中安全导入系统内身份唯一标识以及相关密钥，并在需通行某出入口控制系统时，向出入口控制系统发起身份鉴别，证明身份标识的合法性。机器人相应密码模块提供匹配的密钥或证书存储、使用和管理能力。

5.2 工作流程

5.2.1 生成机器人身份标识

系统为机器人厂商颁发的系统内唯一的厂商标识 UID_M，各机器人厂商再为机器人产生厂商内唯一标识，和厂商标识一起，构成机器人的身份唯一标识符 UID_R。

5.2.2 机器人申请身份鉴别凭证

机器人用 UID_R 生成身份鉴别凭证申请报文，经机器人厂家授权后，向机器人身份生成和分发系统发出申请，机器人身份生成和分发系统确定报文的真实性后，产生与机器人 UID_R 绑定的身份鉴别凭证，并安全导入到相应机器人的密码模块中。

5.2.3 身份鉴别

机器人进行身份鉴别时，首先通过密码模块调用身份鉴别凭证对业务或行为签名，将包含该机器人 UID_R 的签名数据发给出入口控制系统，出入口控制系统收到数据后，通过密码模块调用对应的身份鉴别凭证对数据进行验签以确认 UID_R 的真实性后，利用 UID_R 结合业务需要，确定相应机器人通行权限。

6 与密码相关的安全技术要求

6.1 密码应用安全技术要求

基于机器人通行领域的身份鉴别的密码应用方案宜遵循相应密码算法使用标准，如 GB/T 32905、GB/T 32907、GB/T 35276 等。

6.2 密码设备安全技术要求

基于机器人通行领域身份鉴别的身份生成及分发系统、出入口控制、机器人等，宜使用的密码模块来提供密码各种功能，所有密码设备应具有必要的物理防护措施，以保证密码安全。

6.3 密码功能安全技术要求

系统中要使用的加密、解密功能宜遵循 GB/T 32907；签名、验签等密码功能宜遵循 GB/T 35276。

6.4 密码协议安全技术要求

在系统中，须实现出入口控制系统对机器人的身份鉴别，在身份鉴别过程中所使用的鉴别协议宜遵循 GB/T 15843.2、GB/T 15843.3、GB/T 38636 等。

6.5 密钥管理安全技术要求

6.5.1 密钥生成

系统所需的密钥宜由符合国家密码管理要求的随机数产生，应保证所生成密钥的机密性和随机性。

确保密钥生成过程不可预测，确保在密钥空间内所生成的任意两个密钥具有相同的概率。

6.5.2 密钥的管理

系统所有的密钥注入（如果有）应注意在注入过程中不得泄露明文密钥的任何组成部分；注入过程应在密码设备、接口和传输信道未受到任何可能导致密钥或敏感数据泄露、篡改的状况下，才可以将密钥加载到机器人以及出入口控制系统中。

6.5.3 其他建议

在密钥生成、注入、更新及存储等的整个使用过程中，应保证密钥不被泄漏。

6.6 标识与证书管理

6.6.1 身份标识证书的申请与管理

若采用数字证书方式，机器人在出厂时将其机器人身份标识特征和设备密钥递交给可信的第三方或者自建电子认证服务机构，由电子认证服务机构签发一张能够标识机器人身份的数字证书，数字证书的格式应符合相应的标准，如：GM/T 0015。

当机器人身份标识证书快过期或密码模块核心部件要升级时，需提前发起证书更新；若机器人需要废止使用，可申请身份证书吊销。

6.6.2 统一认证与管理

若采用数字证书方式，可建立统一认证机制，符合要求的第三方或自建电子认证机构可按要求申请并加入统一认证信任源中，集中管理；各机器人厂家向信任源中的各认证服务机构申请的机器人身份证书能够相互认证身份，实现一证通用。

7 密码应用参考方案

本标准给出了以下密码应用方案作为参考。

a） 基于 SM3/SM4 算法身份鉴别的机器人出入口通行方案，参见附录 A；

b） 基于 SM9 算法身份鉴别的机器人出入口通行方案，参见附录 B；

c） 基于数字证书身份鉴别的机器人出入口通行方案，参见附录 C。

8 其他应考虑的安全因素

在本标准中只强调了对密码应用的安全要求，从系统整体的安全性出发，以下因素在具体系统实现时应加以考虑。

a） 后台管理系统的物理环境安全；

b） 管理制度安全；

c） 协商会话密钥；

d） 密钥传输保护；

e） 其他的管理及技术措施，如口令识别、人员值守等。

在系统方案设计及应用时，需针对具体应用情况在密码安全保障的基础上采取其他适当的管理和技术措施，以增强系统的安全性。

附录 A（资料性附录）基于 SM3/SM4 算法身份鉴别的机器人出入口通行方案

A.1 系统构成

本方案采用基于 SM3/SM4 算法身份鉴别的机器人出入口通行方案，系统构成示意图如图 A.1 所示。其中的机器人身份生成和分发系统的核心是 SM4 对称密钥管理系统。

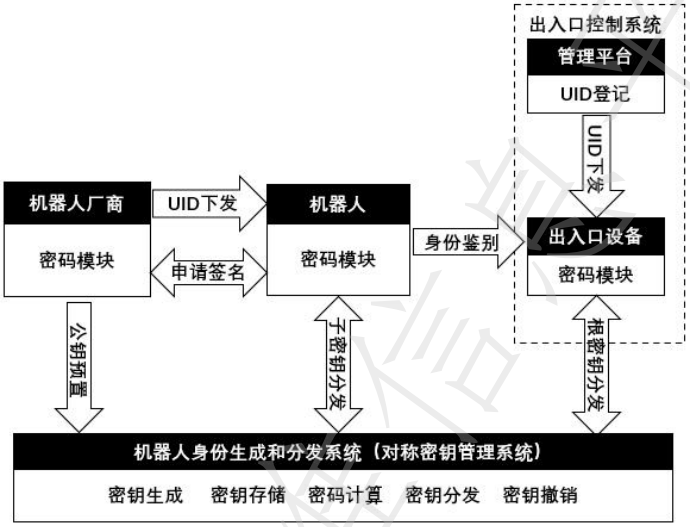

图 A.1 基于 SM3/SM4 算法身份鉴别的机器人出入口控制系统架构图

A.2 应用流程

A.2.1 机器人身份鉴别根密钥的生成

由机器人身份生成及分发系统使用密码模块生成 16 字节长度的机器人身份鉴别根密钥（Keyr）。

A.2.2 各种辅助密钥的生成

辅助密钥的生成，包含以下内容。

a） 由机器人厂家使用密码模块生成 SM2 算法公私钥对：私钥 SK_M、公钥 PK_M；

b） 由机器人使用密码模块产生 SM2 算法的公私钥对：私钥 SK_R、公钥 PK_R。

A.2.3 机器人 UID_R 的生成

机器人 UID_R 的生成，包含以下内容。

a） 由机器人身份生成及分发系统为所有机器人厂家颁发系统内唯一的 4 字节厂商标识 UID_M，用于标记厂家在系统内的唯一性，并将该编号对应的机器人厂家的公钥 PK_M 内置到系统中，与厂家编号绑定；

b） 机器人厂家为每一个机器人生成一个 12 字节的厂家内的唯一编号，用于标记该机器人在厂家内的唯一性；

c） 机器人将 4 字节的厂家编号，加上 12 字节的厂家内唯一编号，构成该机器人系统内唯一的 16

字节身份标识符 UID_R。

A.2.4 机器人身份鉴别子密钥的分发流程

机器人身份鉴别子密钥的分发流程，包含以下内容。

a） 机器人将机器人 UID_R 和公钥 PK_R 形成机器人身份鉴别子密钥请求报文，用机器人厂家私钥 SK_M 签名后，发给机器人身份生成及分发系统；

b） 机器人身份生成及分发系统收到信息后，根据机器人 UID_R 中的厂家编号找到内置在系统中的 PK_M 进行验签，验签通过后，用机器人的 UID_R 对机器人身份鉴别根密钥 Keyr 进行密钥分散，即用密钥 Keyr 对 UID_R 进行一次 SM4 算法加密运算，得出该机器人 UID_R 对应的鉴别子密钥 Keyc；再用 PK_R 对 Keyc 进行 SM2 算法加密后将加密结果发送给机器人；

c） 机器人用对应的私钥 SK_R 从收到的报文中解密该机器人的身份鉴别子密钥 Keyc，并将其安全地导入到密码模块中。

A.2.5 出入口控制系统机器人身份鉴别根密钥的分发流程

分发流程，包含以下内容。

a） 由机器人身份及分发系统发行各出入口控制系统所使用的密码模块，将机器人身份鉴别根密钥安全的导入到各出入口控制系统所使用的密码模块中；

b） 发行的密码模块安装到各出入口控制系统中使用。

A.2.6 机器人登记注册的管理流程

机器人需在管理平台完成登记，将 UID_R 注册到平台并分配相应业务权限，平台将 UID_R 下以及其相对应的业务权限下载到出入口设备中。

A.2.7 机器人身份鉴别

机器人身份鉴别由出入口控制系统来完成，身份鉴别的具体方法如下：

——机器人向出入口控制系统发起身份鉴别流程，将身份唯一标识符（UID_R）、当前时间戳（timestamp）、哈希算法计算的消息认证码（HMACa）一起发送给出入口控制系统。消息认证码（HMACa）是机器人使用一机一密的鉴别密钥（Keyc），采用 SM3 密码杂凑算法对身份标识、机器人当前时间戳进行运算所得，即 HMACa = HMAC(Keyc, UID_R, timestamp)；

——出入口控制器系统在得到机器人上传的信息后，即可以进行机器人的身份鉴别工作，首先利用机器人身份唯一标识符(UID_R)作为分散因子，利用保存在密码模块中的身份鉴别根密钥(Keyr)，用 SM4 算法加密得到机器人的一机一密鉴别密钥（Keyc’），即 Keyc’ = Enc(Keyr, UID_R) 再用此一机一密鉴别密钥（Keyc’）对身份唯一标识符（UID_R）、当前时间戳（timestamp）采用 SM3 算法进行计算消息认证码，即 HMACa’ = HMAC(Keyc’, UID_R, timestamp)，如果 HMACa = HMACa’，且当前时间戳（timestamp）在允许范围内，则机器人身份唯一标识符（UID_R）合法，否则为不合法；

——出入口控制系统将本次鉴别结果发送至机器人。

身份鉴别如图 A.3 所示。

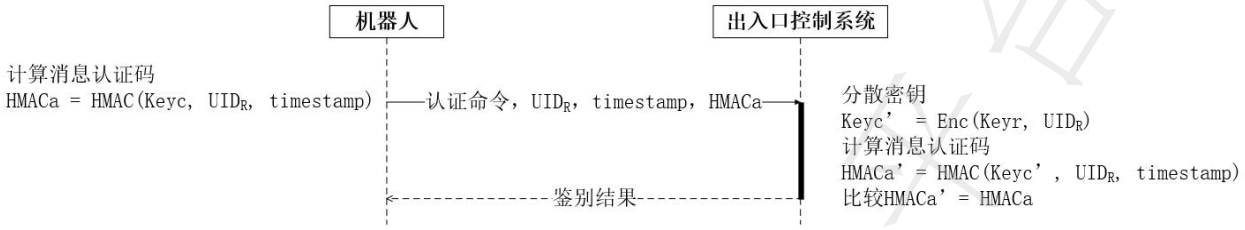

图 A.3 基于出入口控制系统的身份鉴别过程

A.2.8 业务实现

机器人在身份鉴别通过后，通过查询在管理平台中事先登记注册好的机器人白名单，从白名单中取出相应机器人所具有的权限范围，确定机器人是否可进行通行等相关业务操作。

附录 B（资料性附录）基于 SM9 算法身份鉴别的机器人出入口通行方案

B.1 系统构成

本方案采用基于 IBC 身份标识鉴别的机器人出入口通行方案，系统构成示意图如图 B.1 所示。其中的机器人身份生成和分发系统的核心是 IBC 密钥管理系统。

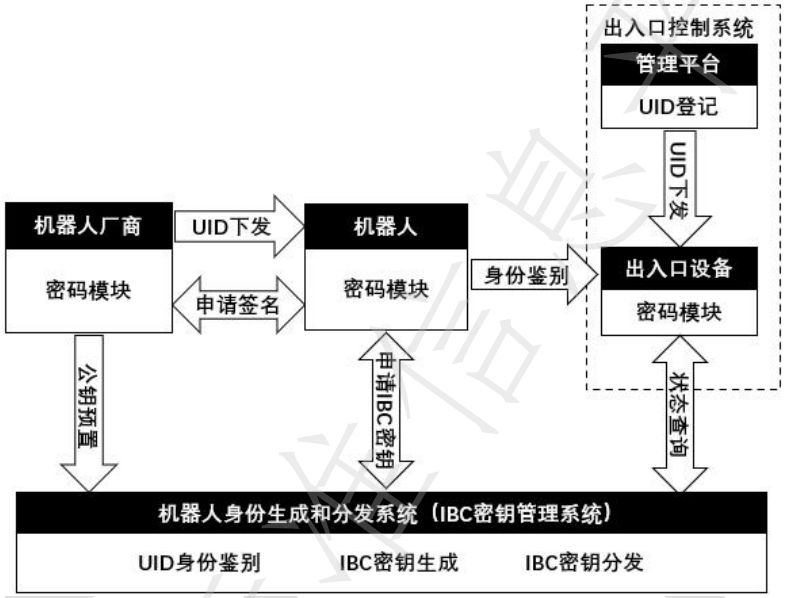

图 B.1 基于 SM9 算法身份鉴别的机器人出入口控制系统架构图

B.2 应用流程

B.2.1 各种辅助密钥的生成

辅助密钥的生成，包含以下内容。

a） 由机器人厂家使用密码模块生成 SM2 算法公私钥对：私钥 SK_M、公钥 PK_M。

b） 由机器人使用密码模块产生 SM2 算法的公私钥对：私钥 SK_R、公钥 PK_R。

B.2.2 机器人 UID_R 的生成

机器人 UID_R 的生成，包含以下内容。

a） 由机器人身份生成及分发系统为所有机器人厂家颁发系统内唯一的 4 字节厂商标识 UID_M，用于标记厂家在系统内的唯一性，并将该编号对应的机器人厂家的公钥 PK_M 内置到机器人身份生成和分发系统中，与厂家编号绑定；

b） 机器人厂家为每一个机器人生成一个 12 字节的厂家内的唯一编号，用于标记该机器人在厂家内的唯一性；

c） 机器人将 4 字节的厂家编号，加上 12 字节的厂家内唯一编号，构成该机器人系统内唯一的 16 字节身份标识符 UID_R。

B.2.3 绑定 UID_R 的 IBC 标识密钥申请流程

密钥申请流程，包含以下内容。

a） 机器人将机器人 UID_R 和公钥 PK_R 形成 IBC 标识密钥请求报文，用机器人厂家私钥 SK_M 签名后，发给机器人身份生成及分发系统；

b） 机器人身份生成及分发系统收到信息后，根据机器人 UID_R 中包含的厂家编号 UID_M 找到内置在系统中的 PK_M 进行验签，验签通过后为此机器人生成其 UID_R 对应的 IBC 标识密钥，并用 PK_R 对 IBC 标识密钥进行 SM2 算法加密后将加密结果发送给机器人；

c） 机器人用私钥 SK_R 从收到的报文中解密该机器人的 IBC 标识密钥，并将其安全地导入到密码模块中。

B.2.4 机器人登记注册的管理流程

机器人需在管理平台完成登记，将 UID_R 注册到平台并分配相应业务权限，平台将 UID_R 下以及其相对应的业务权限下载到出入口设备中。

B.2.5 机器人通行验证流程

机器人向出入口控制器请求通行的身份鉴别机制遵循 GB/T 15843.3 的两次传递鉴别机制。

a） 出入口控制器向机器人发送随机数R_C，并可选地发送一个文本字段$Text1$；

b） 机器人产生并向出入口控制器发送$Token_{MC}$；

c） 出入口控制器在收到$Token_{MC}$后，使用机器人的身份 UID 验证$Token_{MC}$中包含的数字签名；检验$Token_{MC}$中的随机数R_C是否与步骤 a)中发送给机器人的随机数相符；检验$Token_{MC}$中包含的C（如果有）是否等于出入口控制器的可区分标识符。

其中，机器人发送给出入口控制器的$Token_{MC}$的形式如下：

$$Token_{MC} = R_M||R_C||C||Text3||S_{IBC_M}(R_M||R_C||C||Text2)$$

S_{IBC_M}为使用机器人的 IBC 标识密钥对消息的 SM9 签名。

机器人与出入口控制器通讯过程如图 B.3 所示。

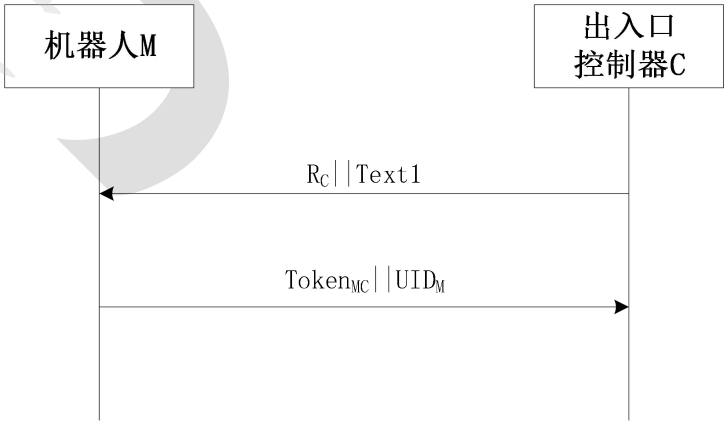

图 B.3 机器人与出入口控制器通讯过程

B.2.6 出入口控制

机器人在身份鉴别通过后，通过查询在管理平台中事先登记注册好的机器人白名单，从白名单中取出相应机器人所具有的权限范围，确定机器人是否可进行通行等相关业务操作。

附录 C（资料性附录）基于数字证书身份鉴别的机器人出入口通行方案

C.1 系统构成

本方案采用基于数字证书身份鉴别的机器人出入口通行方案，系统构成示意图如图 C.1 所示。其中的机器人身份生成和分发系统的核心是 CA 中心，在一些在内部网络中封闭使用的场合，该中心可以是系统自建的证书中心；在公共网络开放使用的场合，要求各个厂家的机器人要能通过各个不同地点、由不同所有者建立的出入口控制系统时，该中心可以是公共的 CA 机构。

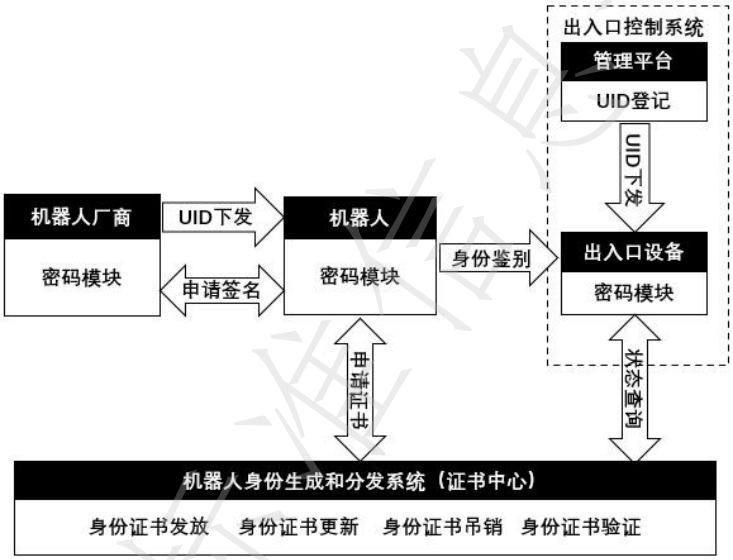

图 C.1 基于数字证书身份鉴别的机器人出入口控制系统架构图

C.2 应用流程

C.2.1 机器人 UID 的生成

机器人 UID_R 的生成，包含以下内容。

a） 机器人身份生成及分发系统为所有机器人厂家颁发系统内唯一的 4 字节厂商标识 UID_M，用于标记该厂家在系统内的唯一性，同时协商相应于该 UID_M 的签名验签方案；

b） 机器人厂家为每一个机器人生成一个 12 字节的厂家内的唯一编号，用于标记该机器人在厂家内的唯一性；

c） 机器人将 4 字节的厂家编号，加上 12 字节的厂家内唯一编号，构成该机器人系统内唯一的 16 字节身份标识符 UID_R。

C.2.2 绑定 UID_R 的身份证书的申请

身份证书申请，包含以下内容。

a） 由机器人使用密码模块产生 SM2 算法的公私钥对：私钥 SK_R、公钥 PK_R，结合 UID_R 产生生成的公钥的身份证书请求文件；

b） 机器人厂家对用之前协商好的签名方案对机器人的请求文件进行签名，发送给机器人身份生成

及分发系统请求颁发身份证书；

c） 机器人身份生成及分发系统收到请求文件后，在文件中包含的UID_R中取出UID_M，并根据UID_M按之前协商好的签名方案对机器人的请求文件进行验签，鉴别UID_M的真实性，确认真实后，并为此机器人设备颁发身份证书。

C.2.3 机器人身份证书的更新或吊销流程

机器人身份证书的更新或吊销流程，包含以下内容。

a） 身份证书更新

机器人可以通过当前有效的证书发起更新申请,机器人身份生成及分发系统验证申请合法后颁发新的证书，更新完成后吊销旧的证书。

b） 身份证书吊销,分为：

1） 自愿吊销：机器人可以通过当前有效的证书发起吊销申请，机器人身份生成及分发系统验证申请合法执行吊销；

2） 强制吊销：当出现特殊情况满足相关要求方执行强制吊销，机器人身份生成及分发系统按业务规则执行。

C.2.4 机器人登记注册的管理流程【待确认管理平台是否需要验证机器人证书合法性】

机器人需在管理平台完成登记，将UID_R注册到平台并分配相应业务权限，平台将UID_R下以及其相对应的业务权限下载到出入口设备中。

C.2.5 机器人通行验证流程

机器人向出入口控制器请求通行的身份鉴别机制遵循 GB/T 15843.3 的两次传递鉴别机制。

a） 出入口控制器向机器人发送随机数R_C，并可选地发送一个文本字段$Text1$。

b） 机器人产生并向出入口控制器发送$Token_{MC}$，并可选地发送机器人的身份证书。

c） 出入口控制器在收到$Token_{MC}$后，执行下列步骤：

1） 向管理平台请求验证机器人的身份证书，验证内容包括：是否在有效期内、是否由可信 CA 证书机构颁发、是否被吊销、证书密钥用法是否正确等；

2） 利用机器人的身份证书验证$Token_{MC}$中包含的数字签名；检验$Token_{MC}$中的随机数R_C是否与步骤 1)中发送给机器人的随机数相符；检验$Token_{MC}$中包含的C（如果有）是否等于出入口控制器的可区分标识符。

其中，机器人发送给出入口控制器的$Token_{MC}$的形式如下：

$$Token_{MC} = R_M||R_C||C||Text3||S_{S_M}(R_M||R_C||C||Text2)$$

机器人与出入口控制器通讯过程如图 C.3 所示。

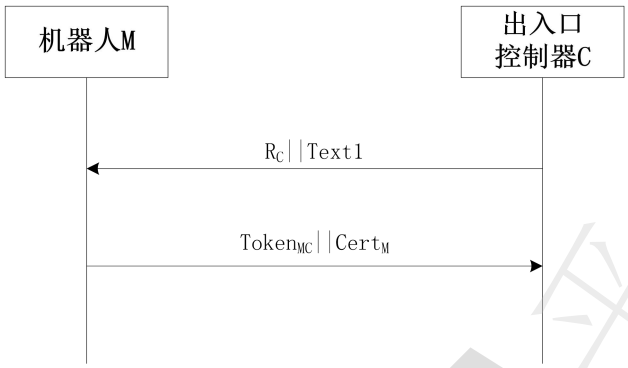

图 C.3 机器人与出入口控制器通讯过程

C.2.6 出入口控制

机器人在身份鉴别通过后，通过查询在管理平台中事先登记注册好的机器人白名单，从白名单中取出相应机器人所具有的权限范围，确定机器人是否可进行通行等相关业务操作。