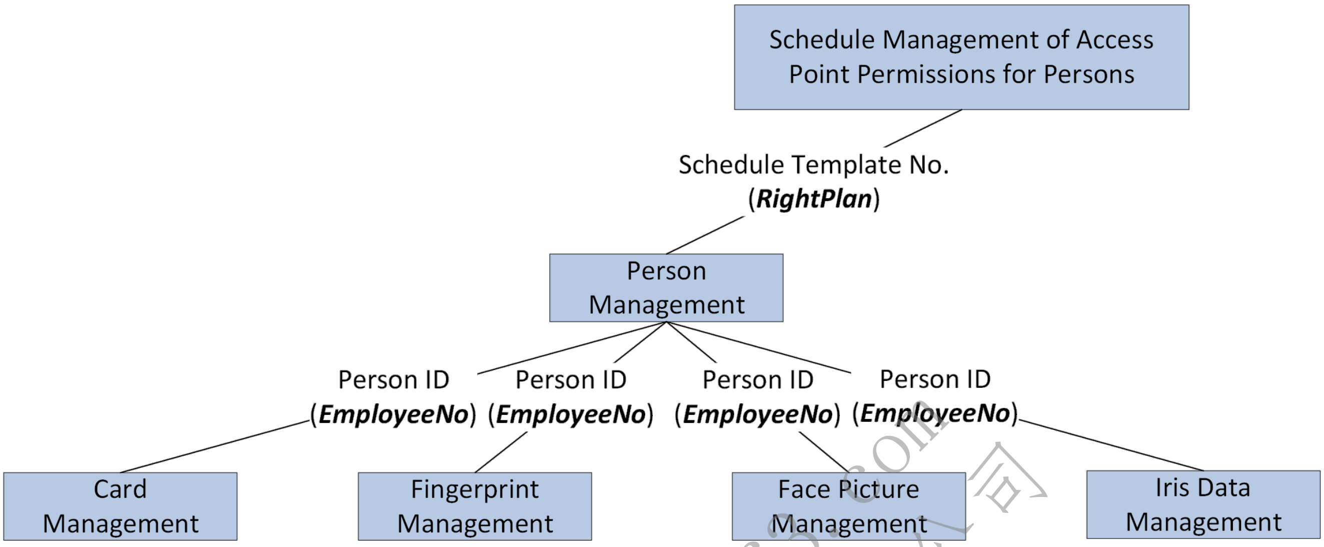
9.14 Person and Credential Management

9.14.1 Introduction to the Function

The person and credential management function is person-based, and is for managing persons, credentials (cards, fingerprints, face pictures, and iris data), and permission schedules which control the permissions for persons to enter and exit the controlled areas. Its architecture is shown below.



This document mainly introduces the calling flows for person management and credential management (card, fingerprint, face picture, iris data management). For details about the calling flow for permission schedule management, refer to the “Management of Permission Schedules for Persons and Access Points”.

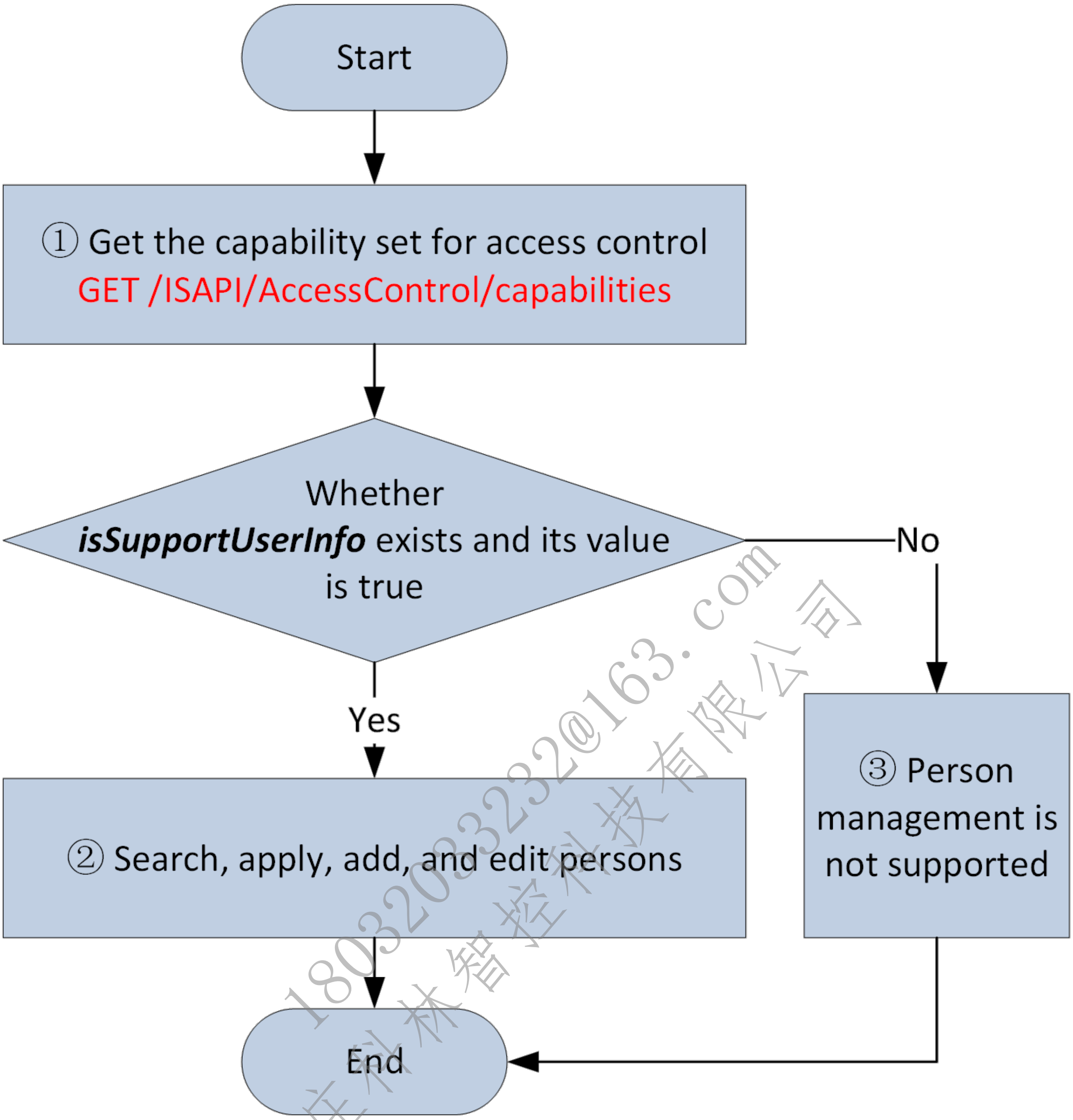
9.15 Person Management

9.15.1 Introduction to the Function

Person management includes searching, applying, adding, editing, and deleting persons.

9.15.2 API Calling Flow

9.15.2.1 Check Whether the Device Supports Person Management


Start
① Get the capability set for access control
GET /ISAPI/AccessControl/capabilities
Whether
isSupportUserInfo exists and its value is true
No
Yes
② Search, apply, add, and edit persons
③ Person management is not supported
End

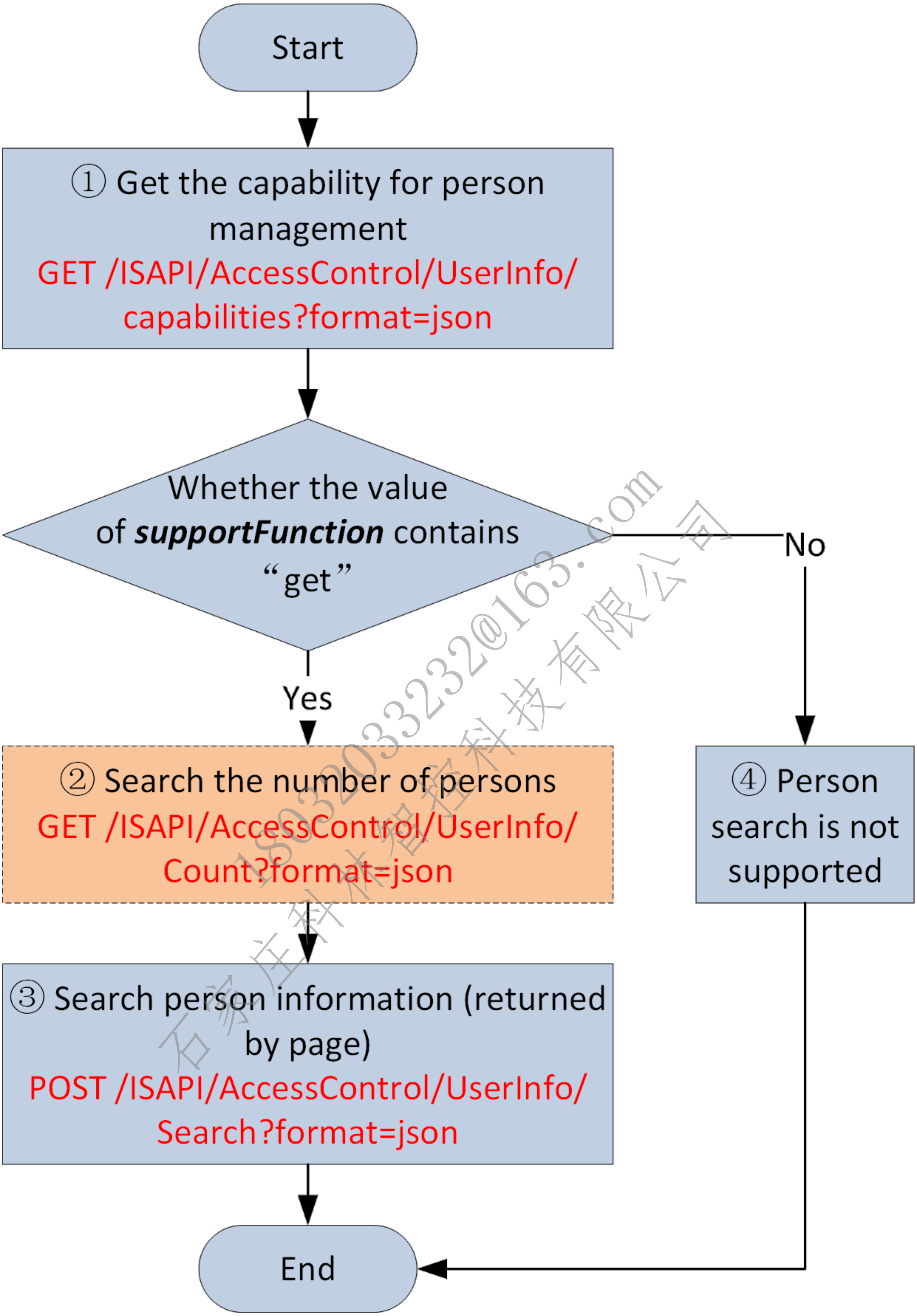
Before calling the API for person management, make sure that the device supports person management.

1. Check whether the device supports person management: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportUserInfo is returned and its value is true, it indicates that the device supports person management.
2. Search, apply, add, and edit persons.
3. If the node isSupportUserInfo is returned and its value is false, it indicates that the device does not support person management.

Note:

The person ID (EmployeeNo) is the unique identifier for person and credential management. After calling `GET /ISAPI/AccessControl/capabilities`, through the child nodes of EmployeeNoInfo which are employeeNo, characterType, and isSupportCompress, the maximum string length and character types of the person ID supported by the device can be checked. Generally, devices support up to 32 bytes and any type of characters. But for access controllers and distribution-type access control devices, check through the child nodes mentioned above.

9.15.2.2 Person Search


Start
① Get the capability for person management
GET /ISAPI/AccessControl/UserInfo/capabilities?format=json
Whether the value of *supportFunction* contains "get"
No
Yes
② Search the number of persons
GET /ISAPI/AccessControl/UserInfo/Count?format=json
④ Person search is not supported
③ Search person information (returned by page)
POST /ISAPI/AccessControl/UserInfo/Search?format=json
End

The person search function is for searching the number of persons and person information added to the device.

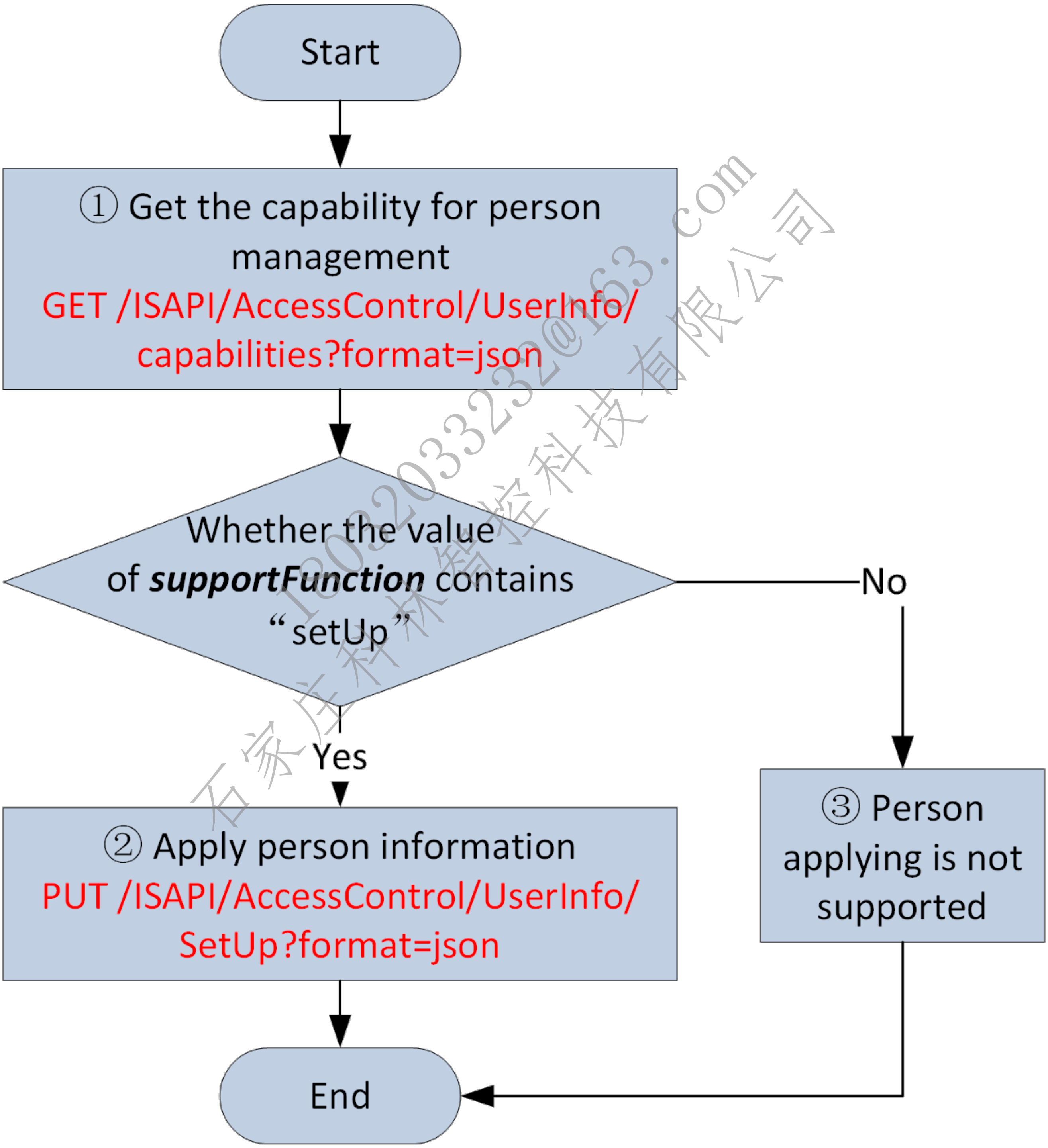
1. Check whether the device supports person search: `GET /ISAPI/AccessControl/UserInfo/capabilities?format=json`; if the value of the node supportFunction contains "get", it indicates that the device supports person search.

2. Search the number of persons: `GET /ISAPI/AccessControl/UserInfo/Count?format=json`; the returned value of the node userNumber is the number of the persons added to the device.
3. Search person information: `POST /ISAPI/AccessControl/UserInfo/Search?format=json`; the person information is returned by page.
4. If the value of the node supportFunction does not contain "get", it indicates that the device does not support person search.

Note:

The value of the node maxRecordNum returned by calling `GET /ISAPI/AccessControl/UserInfo/capabilities?format=json` is the maximum number of persons supported by the device.

9.15.2.3 Person Applying


Start
① Get the capability for person management
GET /ISAPI/AccessControl/UserInfo/capabilities?format=json
Whether the value of *supportFunction* contains "setUp"
No
Yes
② Apply person information
PUT /ISAPI/AccessControl/UserInfo/SetUp?format=json
③ Person applying is not supported
End

Person information can be applied to the device via the person applying function. If the person has been added to the device, the person information will be edited; if the person has not been added to the device, the person information will be applied to the device.

1. Check whether the device supports person applying: `GET /ISAPI/AccessControl/UserInfo/capabilities?`

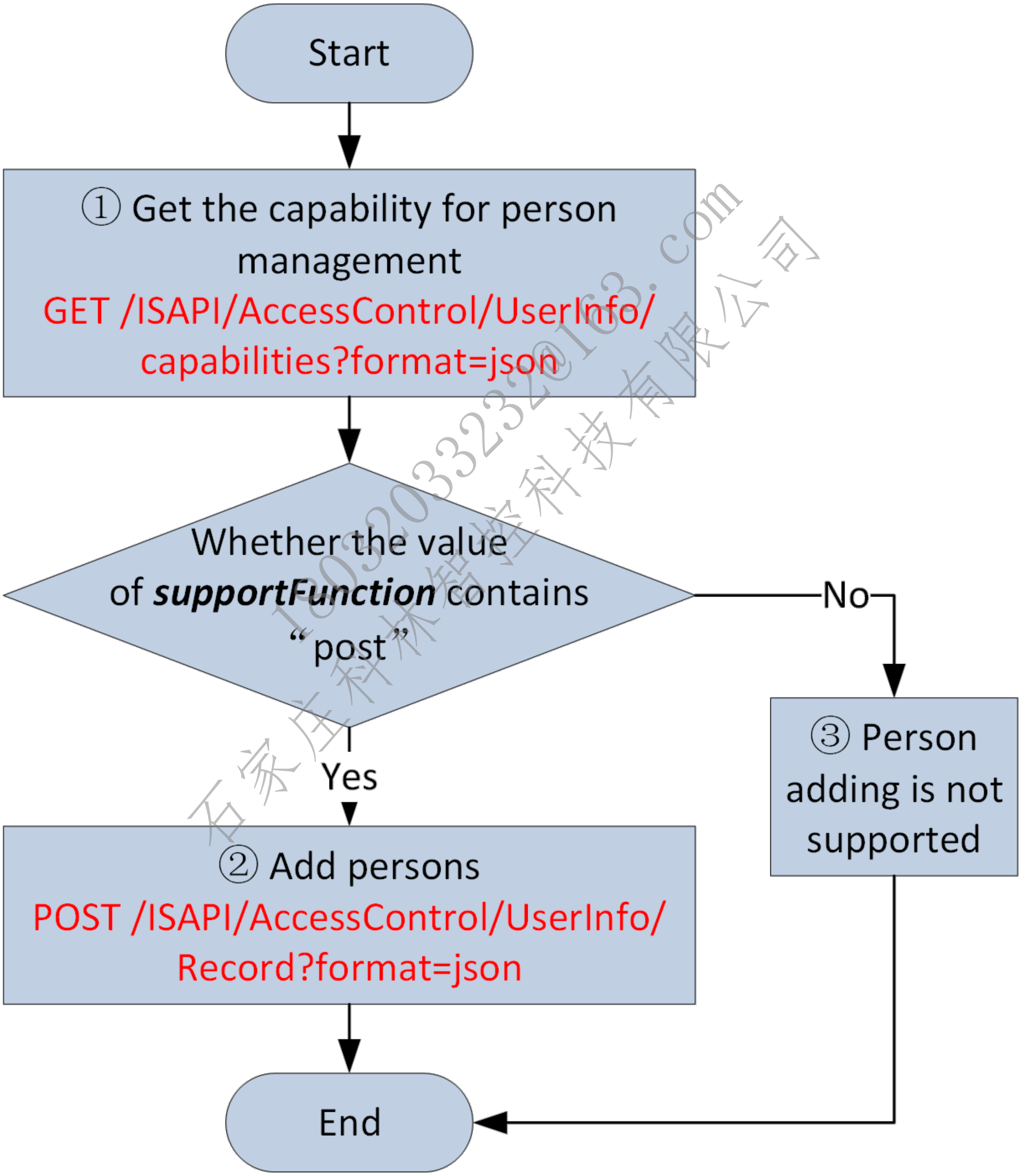
`format=json`; if the value of the node supportFunction contains “setUp”, it indicates that the device supports person applying.

2. Apply person information: `PUT /ISAPI/AccessControl/UserInfo/SetUp?format=json`.
3. If the value of the node supportFunction does not contain setUp, it indicates that the device does not support person applying.

Note:

Check whether the person has been added to the device via the node employeeNo returned after calling the API for person applying.

9.15.2.4 Person Adding


Start
① Get the capability for person management
GET /ISAPI/AccessControl/UserInfo/capabilities?format=json
Whether the value of *supportFunction* contains “post”
No
Yes
② Add persons
POST /ISAPI/AccessControl/UserInfo/Record?format=json
③ Person adding is not supported
End

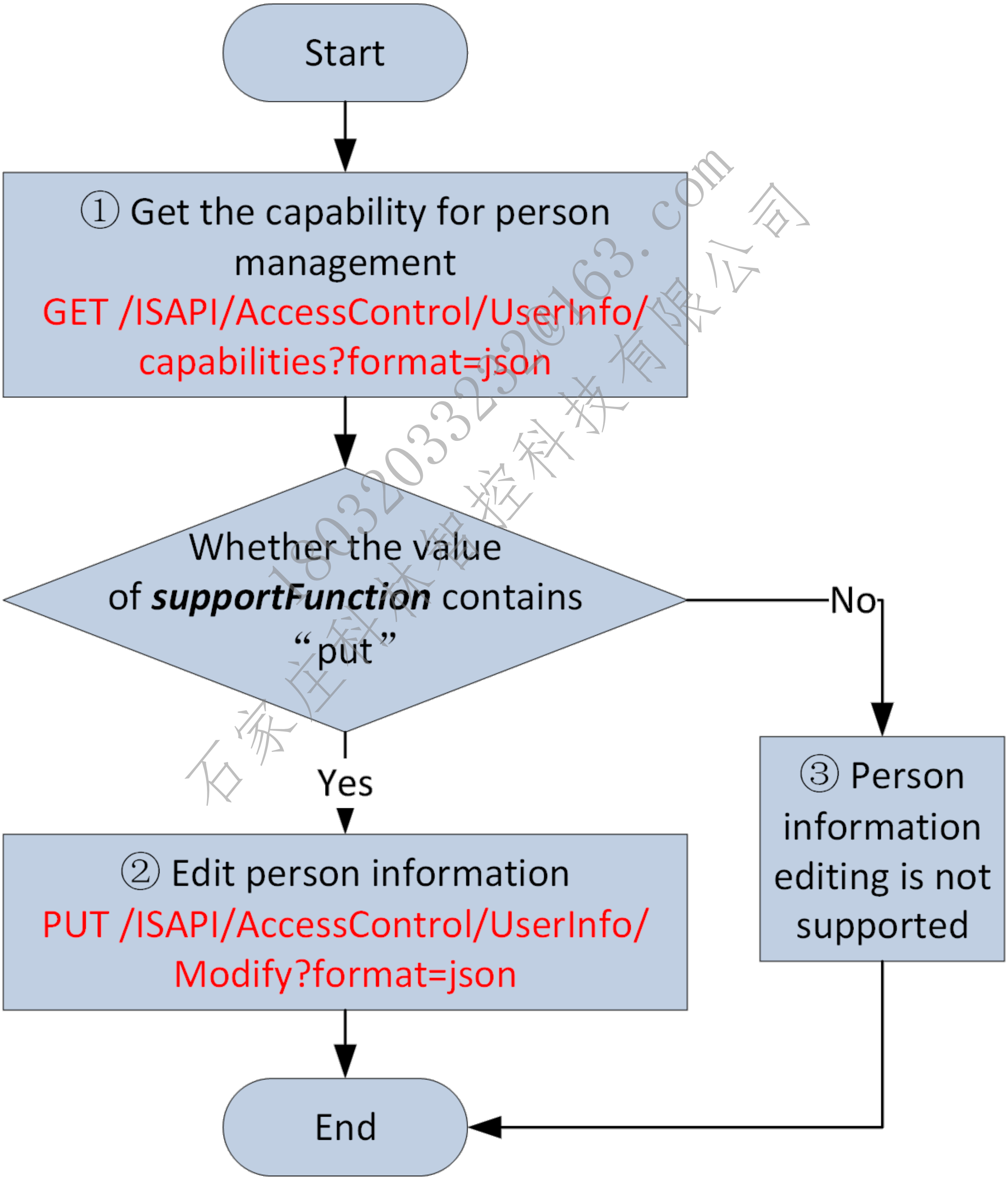
Person can be added to the device via the person adding function. If the person has been added to the device, the device will report an error; if the person has not been added to the device, the person will be added to the device.

1. Check whether the device supports person adding: `GET /ISAPI/AccessControl/UserInfo/capabilities?format=json`; if the value of the node supportFunction contains “post”, it indicates that the device supports person adding.
2. Add persons: `POST /ISAPI/AccessControl/UserInfo/Record?format=json`.
3. If the value of the node supportFunction does not contain “post”, it indicates that the device does not support person adding.

Note:

Check whether the person has been added to the device via the node employeeNo returned after calling the API for person adding.

9.15.2.5 Person Information Editing


Start
① Get the capability for person management
GET /ISAPI/AccessControl/UserInfo/capabilities?format=json
Whether the value of *supportFunction* contains “put”
No
Yes
② Edit person information
PUT /ISAPI/AccessControl/UserInfo/Modify?format=json
③ Person information editing is not supported
End

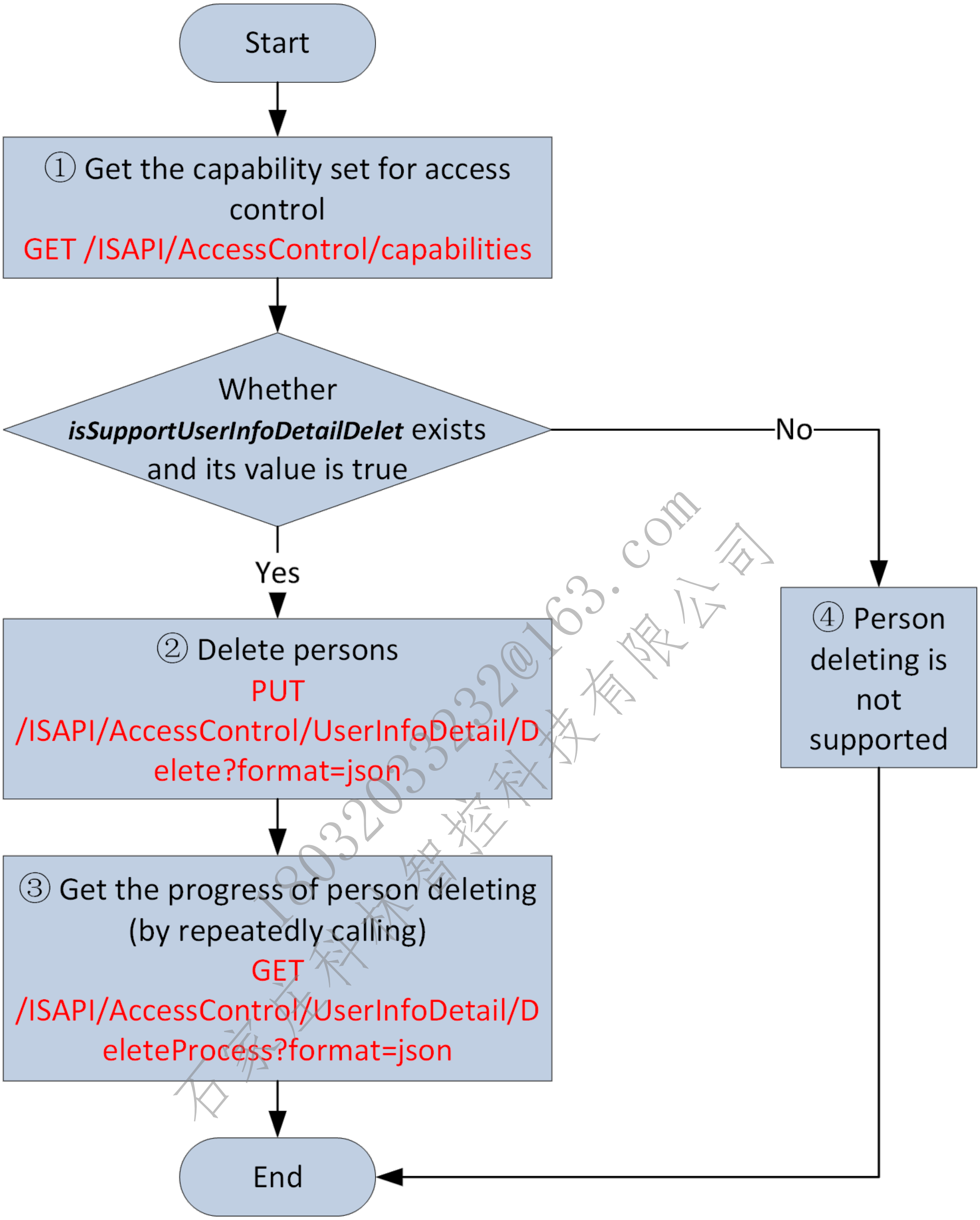
Person information added to the device can be edited via the person information editing function. If the person has been added to the device, the person information will be edited; if the person has not been added to the device, the device will report an error.

1. Check whether the device supports person information editing: `GET /ISAPI/AccessControl/UserInfo/capabilities?format=json`; if the value of the node supportFunction contains "put", it indicates that the device supports person information editing.
2. Edit Person Information: `PUT /ISAPI/AccessControl/UserInfo/Modify?format=json`.
3. If the value of the node supportFunction does not contain "put", it indicates that the device does not support person information editing.

Note:

Check whether the person has been added to the device via the node employeeNo returned after calling the API for person information editing.

9.15.2.6 Person Deleting


Start
① Get the capability set for access control
GET /ISAPI/AccessControl/capabilities
Whether *isSupportUserInfoDetailDelet* exists and its value is true
No
Yes
② Delete persons
PUT /ISAPI/AccessControl/UserInfoDetail/Delete?format=json
③ Get the progress of person deleting (by repeatedly calling)
GET /ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json
④ Person deleting is not supported
End

The person added to the device can be deleted via the person deleting function. The device will not report an error if the person to be deleted is not added to the device.

1. Check whether the device supports person deleting: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportUserInfoDetailDelete is returned and its value is “true”, it indicates that the device supports person deleting.
2. Delete persons: `PUT /ISAPI/AccessControl/UserInfoDetail/Delete?format=json`; if calling succeeded, it indicates that the device has started to execute person deleting, but it does not indicate that the device has deleted the person.
3. Get the progress of deleting person information: `GET /ISAPI/AccessControl/UserInfoDetail/DeleteProcess`; repeatedly call this API to get the progress of person deleting.
4. If the node isSupportUserInfoDetailDelete is returned and its value is “false”, it indicates that the device does not

support person deleting.

Note:

When the person is deleted, the information on the credentials (the card, fingerprint, face picture, and iris data) linked via the person ID will also be deleted.

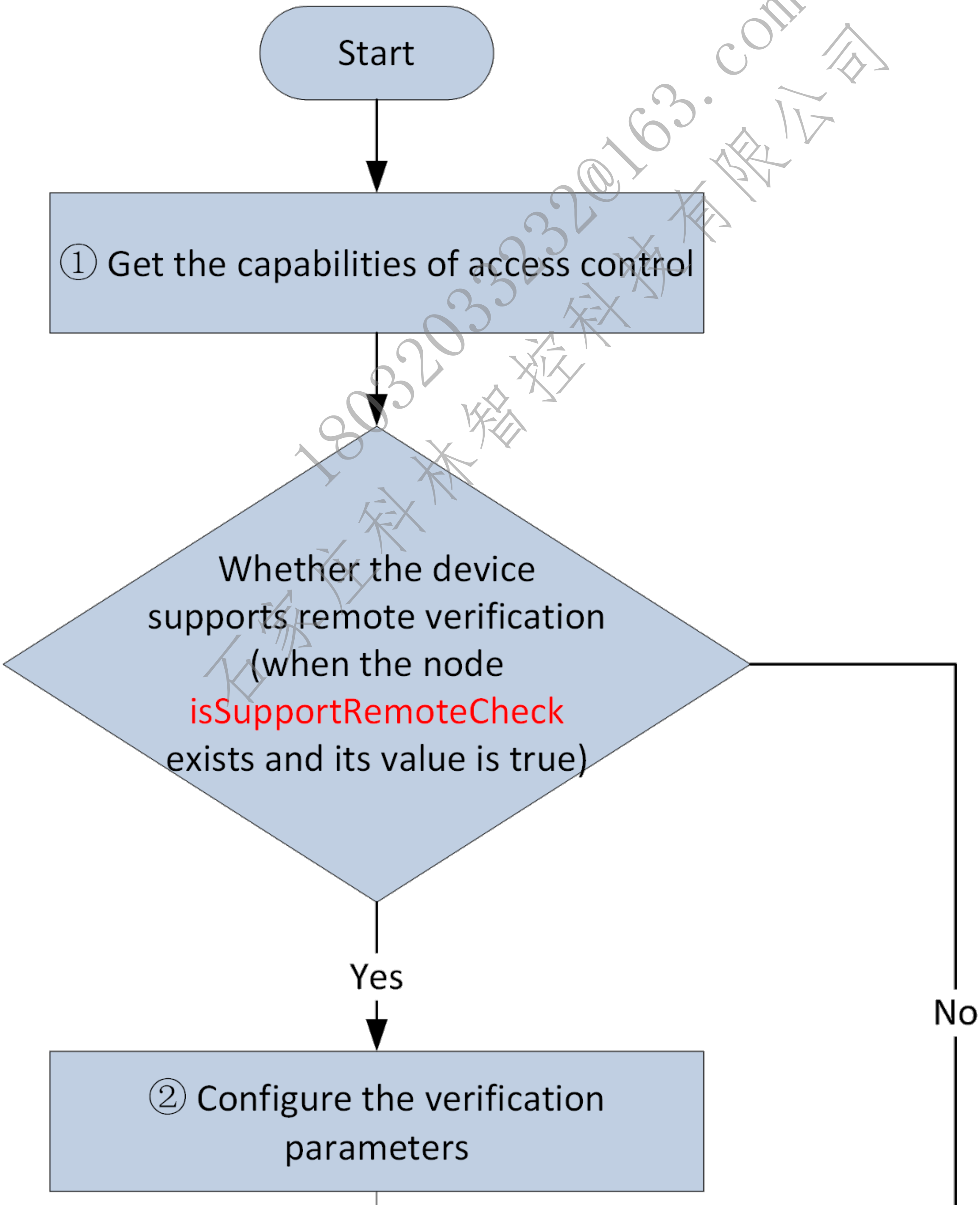
9.16 Remote Verification

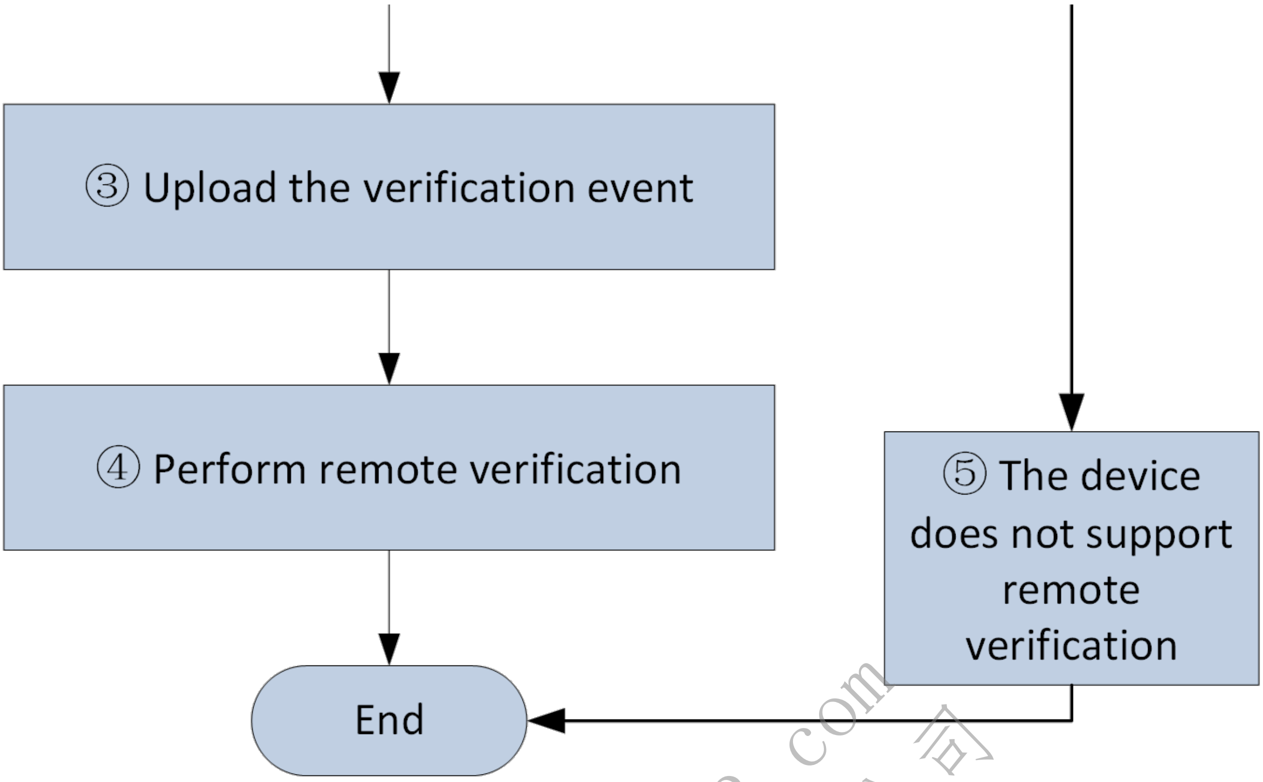
9.16.1 Introduction to the Function

For scenes with high-level security/protection requirements, it requires not only the device's local authentication but also the platform's verification before enabling door controlling.

For example, in scenes such as pandemic control and prevention, after completing authentication/temperature measurement of the person, the device will upload the event to the platform, and the platform will search for the person's recent trip information according to the uploaded information and apply the verification result to the device for controlling door after confirming the person's trip does not involve risk areas.

9.16.2 API Calling Flow


Start
① Get the capabilities of access control
Whether the device supports remote verification (when the node isSupportRemoteCheck exists and its value is true)
Yes
No
② Configure the verification parameters


③ Upload the verification event
④ Perform remote verification
⑤ The device does not support remote verification
End

The API calling flow is as follow:

1. Check whether the device supports remote verification: `GET /ISAPI/AccessControl/capabilities`. If the node isSupportRemoteCheck is returned and its value is true, it indicates that the device supports remote verification.
2. Configure verification parameters: `[GET/PUT] /ISAPI/AccessControl/AcsCfg?format=json`; configure the verification parameters via the nodes including remoteCheckDoorEnabled, checkChannelType, channelIp and needDeviceCheck.
3. Upload events to be verified: when the node remoteCheck of the following events (AccessControllerEvent/ IDCardInfoEvent/ QRCodeEvent/ FaceTemperatureMeasurementEvent) is returned and its value is true, it indicates that this event requires remote verification.
4. Perform remote verification: `PUT /ISAPI/AccessControl/remoteCheck?format=json`. Apply remote verification result.
5. Remote verification is not supported by this device.

9.17 Reset Anti-Passback Rule (Additional Function)

9.17.1 Introduction to the Function

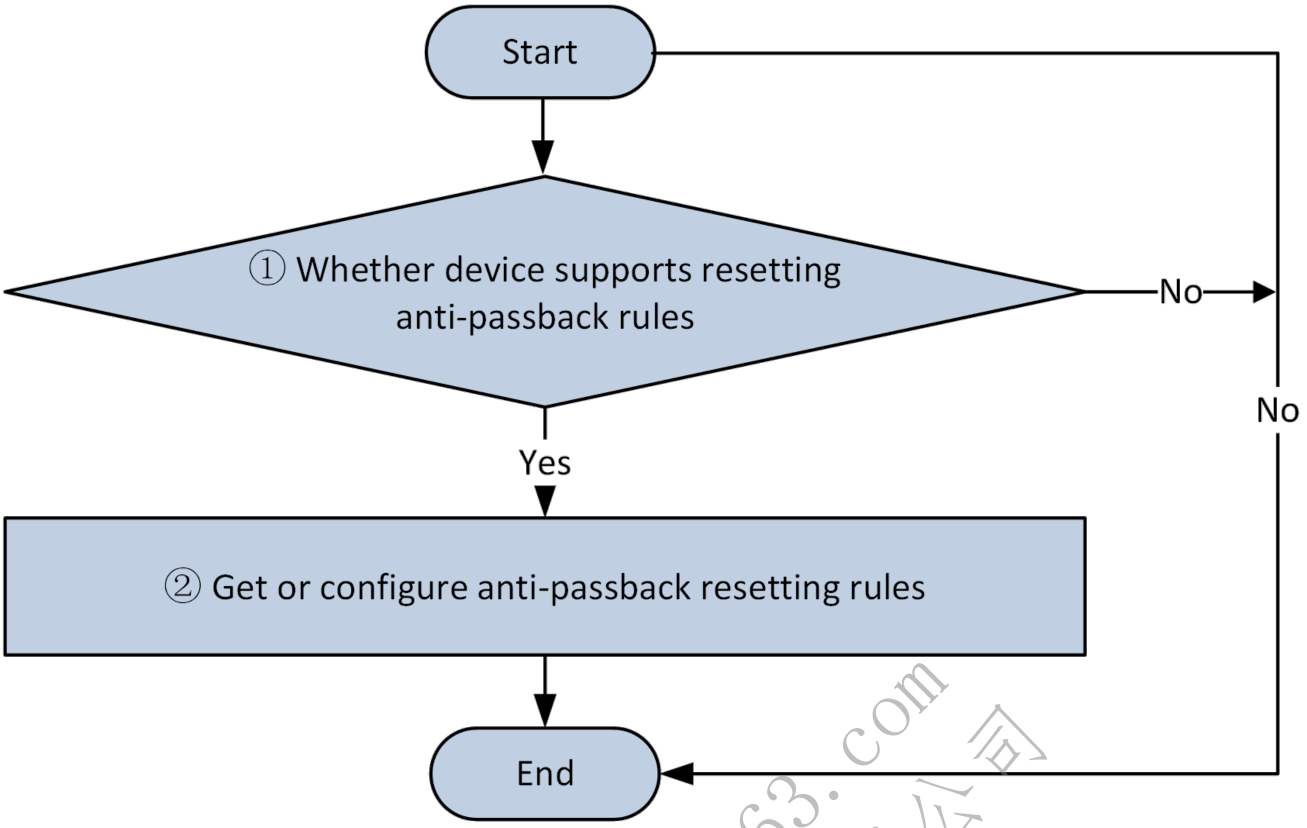
Anti-passback rules which can be reset:

1. Reset by authentication interval. This function will take effect in specific time period after the anti-passbak is triggered. If the user trigger the function by swiping a card by route, the anti-passback flag will be reset in certain time.
2. Reset by time. The anti-passback flag will be reset automatically in certain time.
3. Invalid mode. The resetting rule is disabled.

Application scenarios: The anti-passback function will be help to reduce the cost of manual monitoring. Anti-passback by time period and by time cannot set at the same time.

9.17.2 API Calling Flow

Calling Flow:


Start
① Whether device supports resetting anti-passback rules
No
No
Yes
② Get or configure anti-passback resetting rules
End

ISAPI Protocol Calling Flow:

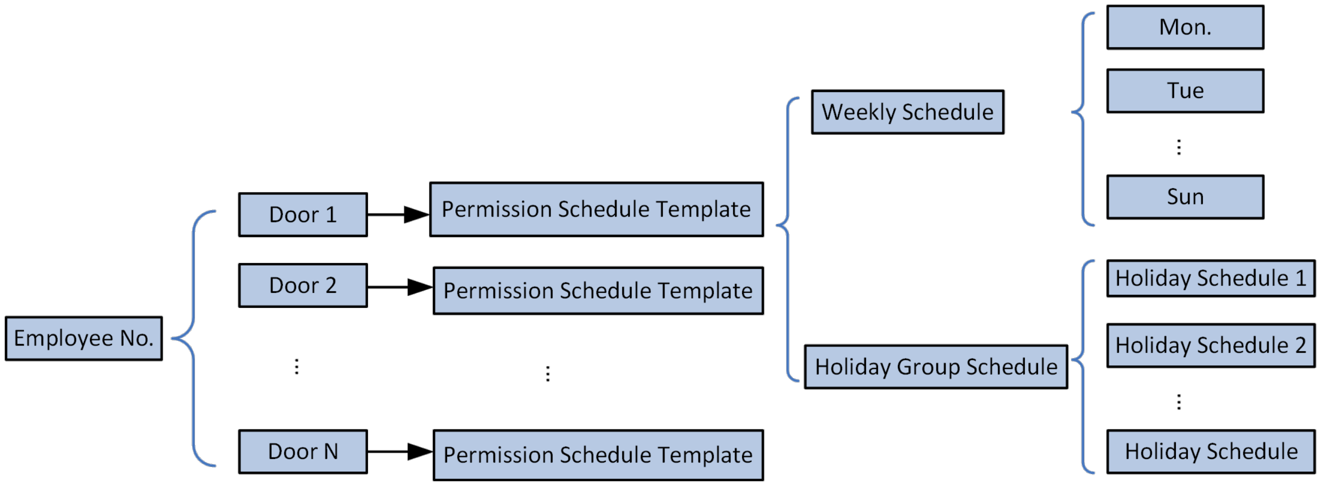
1. Get the capability of access control: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportAntiPassbackResetRules is returned and its value is "true", it indicates that the device supports resetting rules of anti-passback.
2. Get resetting rules of anti-passback: `GET /ISAPI/AccessControl/AntiPassback/resetRules?format=json`; configure resetting rules of anti-passback: `PUT /ISAPI/AccessControl/AntiPassback/resetRules?format=json`.

9.18 Schedules Management of Persons' Access Permission

9.18.1 Introduction to the Function

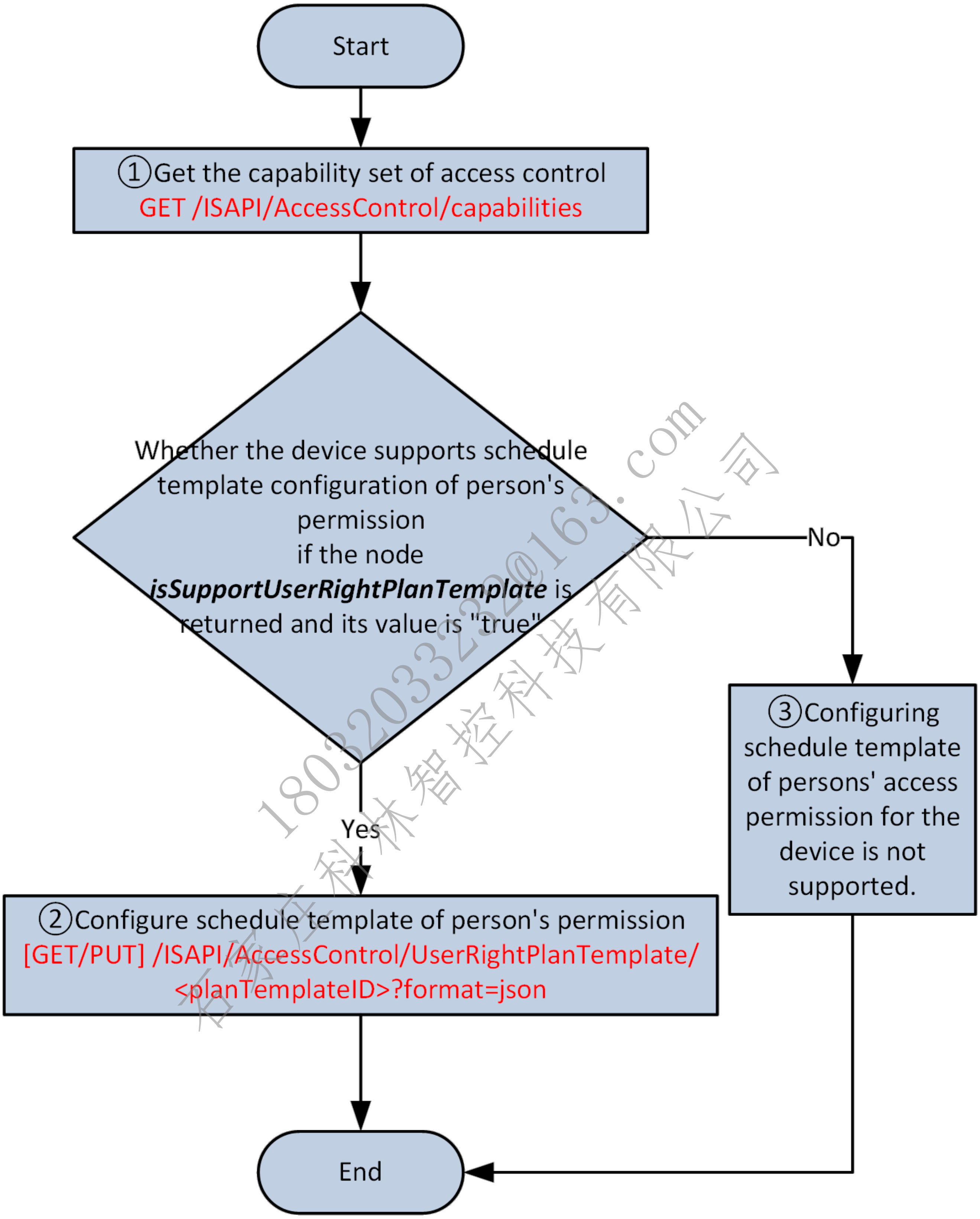
It is required to connect to door permission and schedule template of access permission related to each door before applying permissions to persons. For applying permissions to persons, see calling flow of *Person Management* of *Person and Credential Management*. Configuring schedules of persons' access permission is required, or the related persons cannot access.

1 weekly schedule and 4 holiday groups can be added in each schedule template. The priority of holiday schedule is higher than that of weekly schedule. Weekly schedule can be configured by day of a week and 8 different time period of a day. 16 holiday schedules can be added to a holiday group schedule. Each holiday schedule has its start and end day, and the time period is same in the holiday range (8 time periods can be added). The access control can follow the schedule template to manage person's permissions by time.



9.18.2 API Calling Flow

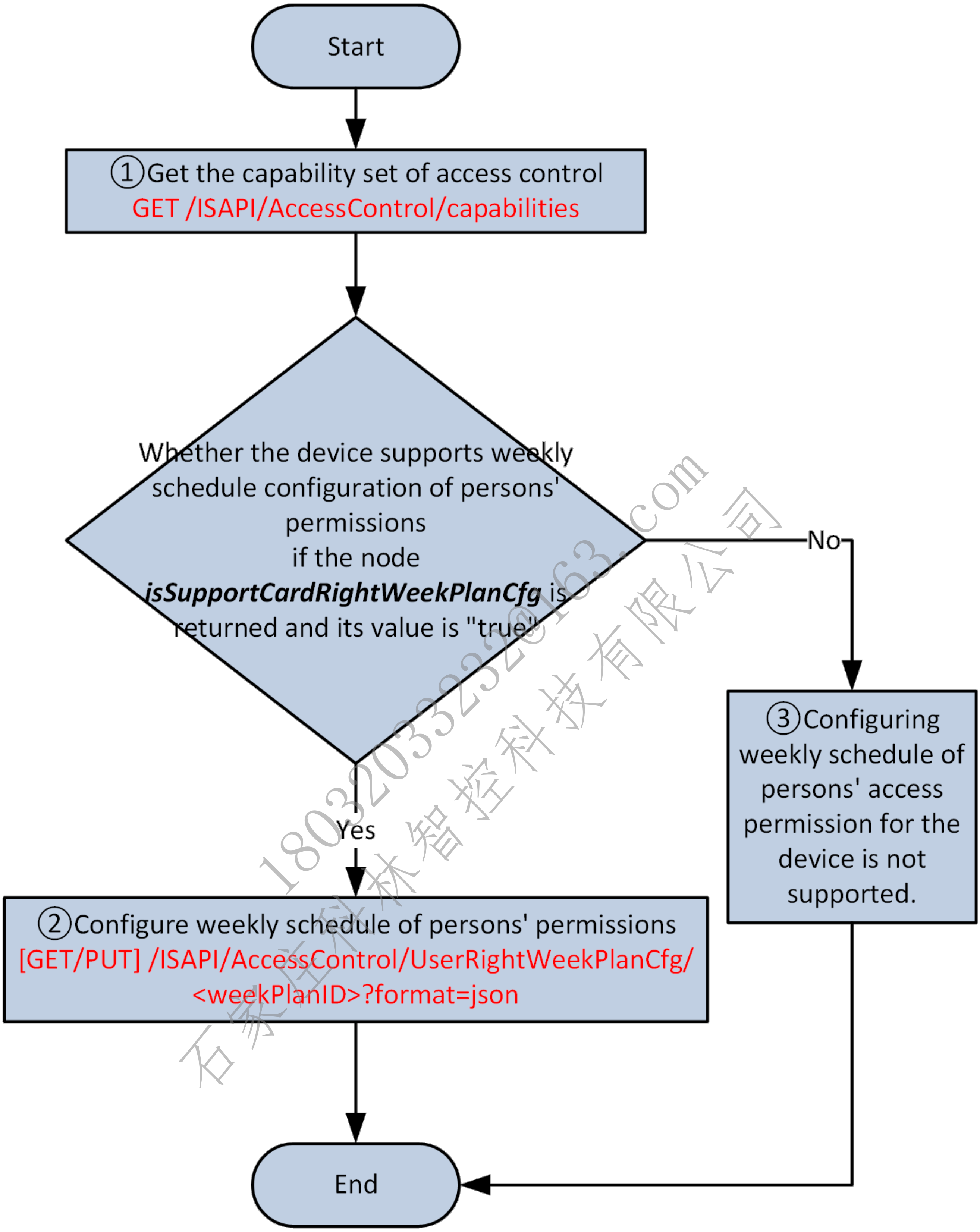
9.18.2.1 Schedule Template of Persons' Access Permission


Start
①Get the capability set of access control
GET /ISAPI/AccessControl/capabilities
Whether the device supports schedule template configuration of person's permission
if the node *isSupportUserRightPlanTemplate* is returned and its value is "true"
No
Yes
②Configure schedule template of person's permission
[GET/PUT] /ISAPI/AccessControl/UserRightPlanTemplate/<planTemplateID>?format=json
③Configuring schedule template of persons' access permission for the device is not supported.
End

Calling Flow:

1. Check whether the device supports schedule template configuration of person's permission: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportUserRightPlanTemplate is returned and its value is "true", it indicates that the device supports schedule template configuration of person's permission (if it supports, it also supports weekly schedule configuration of persons' permission).
2. Schedule template configuration of persons' permission: `[GET/PUT] /ISAPI/AccessControl/UserRightPlanTemplate/<planTemplateID>?format=json`.
3. Configuring schedule template of persons' access permission control for the device is not supported.

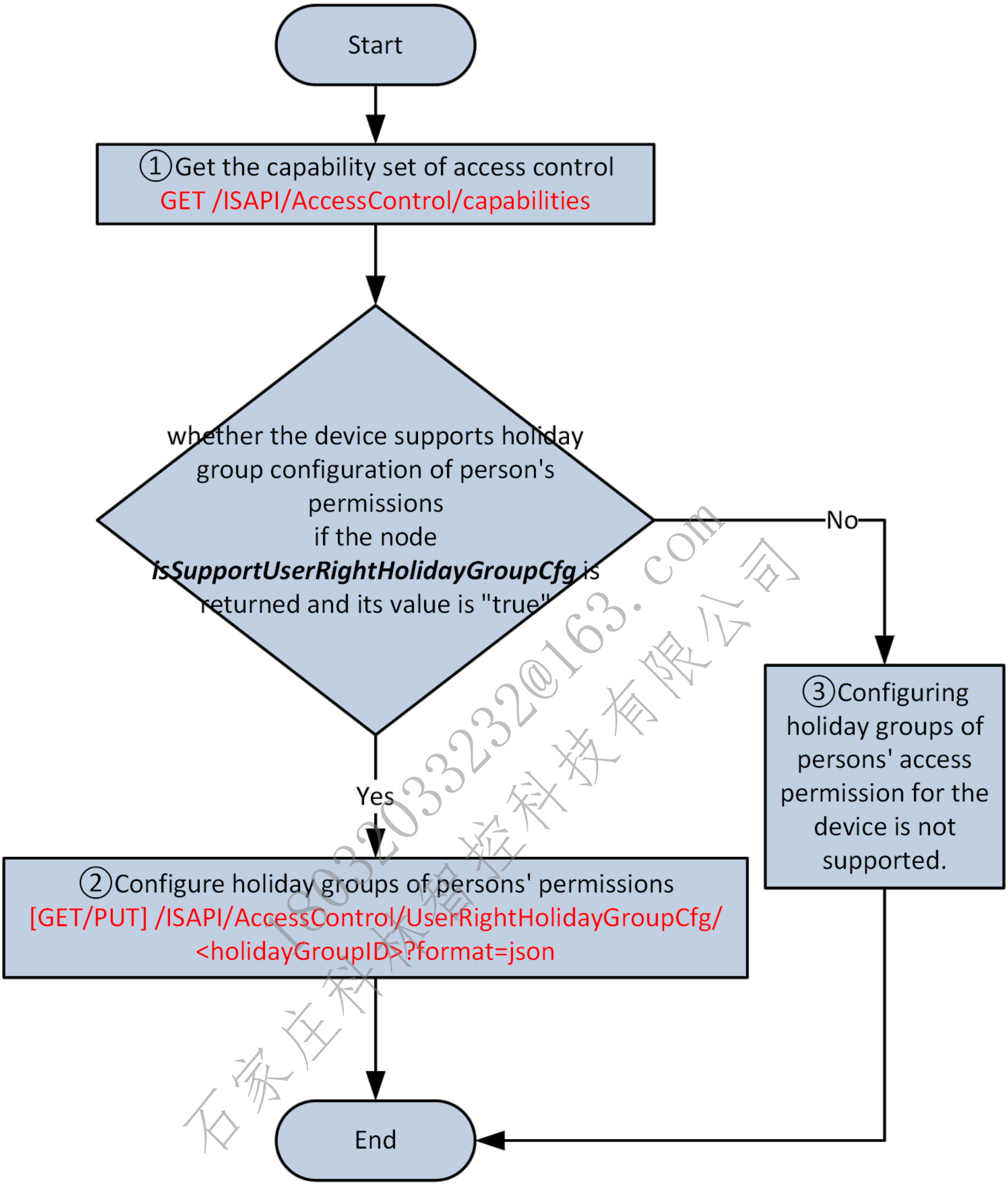
9.18.2.2 Weekly Schedule of Persons' Access Permission


Start
①Get the capability set of access control
GET /ISAPI/AccessControl/capabilities
Whether the device supports weekly schedule configuration of persons' permissions
if the node *isSupportCardRightWeekPlanCfg* is returned and its value is "true"
No
Yes
③Configuring weekly schedule of persons' access permission for the device is not supported.
②Configure weekly schedule of persons' permissions
[GET/PUT] /ISAPI/AccessControl/UserRightWeekPlanCfg/<weekPlanID>?format=json
End

Calling Flow:

1. Check whether the device supports weekly schedule configuration of persons' permissions: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportCardRightWeekPlanCfg is returned and its value is "true", it indicates that the device supports weekly schedule configuration of person's permissions.
2. Weekly schedule configuration of persons' permissions:`[GET/PUT] /ISAPI/AccessControl/UserRightWeekPlanCfg/<weekPlanID>?format=json`.
3. Configuring weekly schedule of persons' access permission control for the device is not supported.

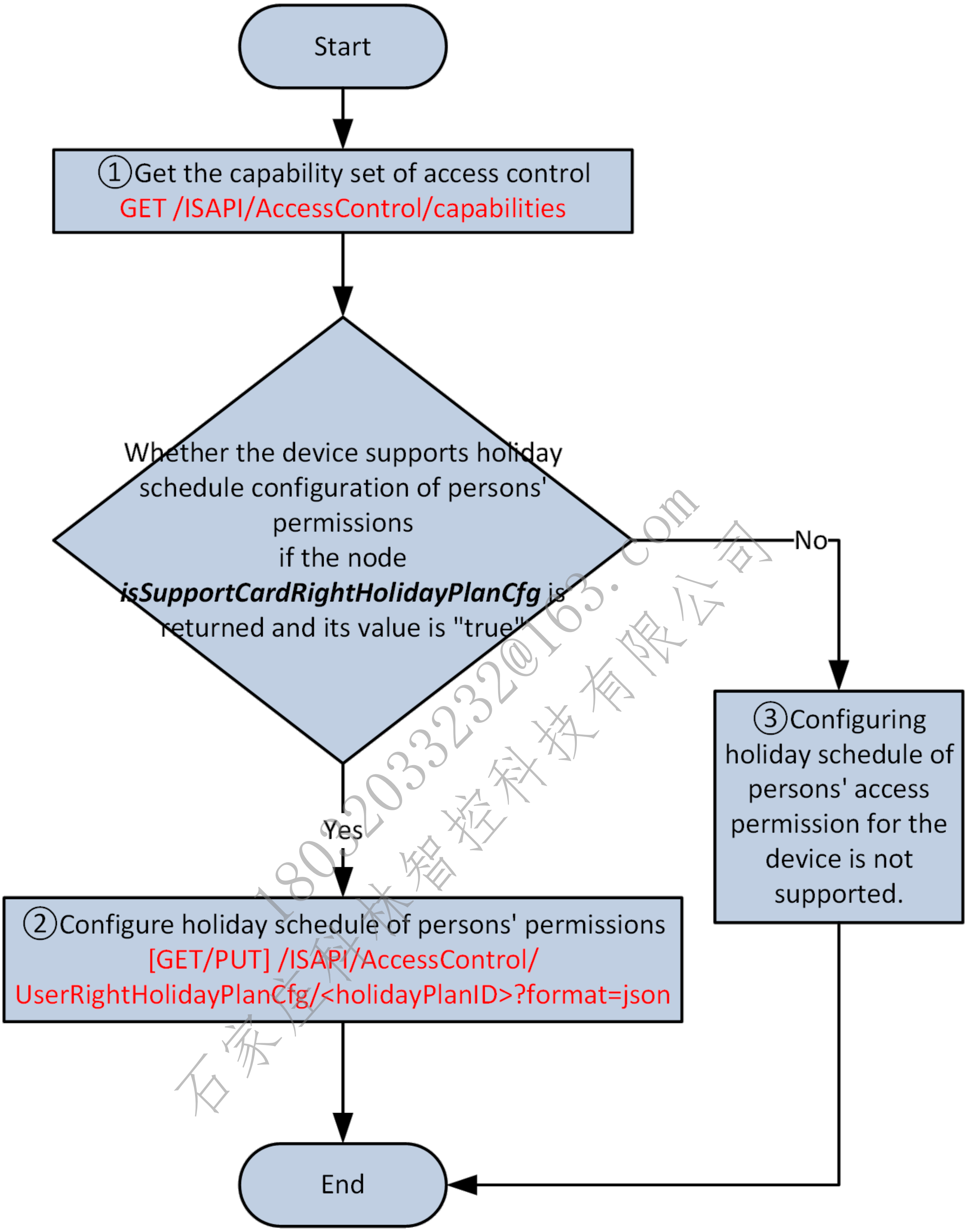
9.18.2.3 Holiday Groups of Persons' Access Permission


Start
①Get the capability set of access control
GET /ISAPI/AccessControl/capabilities
whether the device supports holiday group configuration of person's permissions
if the node *isSupportUserRightHolidayGroupCfg* is returned and its value is "true"
No
Yes
②Configure holiday groups of persons' permissions
[GET/PUT] /ISAPI/AccessControl/UserRightHolidayGroupCfg/<holidayGroupID>?format=json
③Configuring holiday groups of persons' access permission for the device is not supported.
End

Calling Flow:

1. Check whether the device supports holiday group configuration of person's permissions: `GET /ISAPI/AccessControl/capabilities`; if the nodeisSupportUserRightHolidayGroupCfg is returned and its value is "true", it indicates that the device supports holiday group configuration of person's permission (if it supports, it also supports holiday schedule configuration of persons' permissions).
2. Holiday group configuration of persons' permissions:`[GET/PUT] /ISAPI/AccessControl/UserRightHolidayGroupCfg/<holidayGroupID>?format=json`.
3. Configuring holiday groups of persons' access permission control for the device is not supported.

9.18.2.4 Holiday Schedule of Persons' Access Permission


Start
①Get the capability set of access control
GET /ISAPI/AccessControl/capabilities
Whether the device supports holiday schedule configuration of persons' permissions
if the node *isSupportCardRightHolidayPlanCfg* is returned and its value is "true"
No
Yes
②Configure holiday schedule of persons' permissions
[GET/PUT] /ISAPI/AccessControl/UserRightHolidayPlanCfg/<holidayPlanID>?format=json
③Configuring holiday schedule of persons' access permission for the device is not supported.
End

Calling Flow:

1. Check whether the device supports holiday schedule configuration of persons' permissions: `GET /ISAPI/AccessControl/capabilities`; if the node isSupportCardRightHolidayPlanCfg is returned and its value is "true", it indicates that the device supports holiday schedule configuration of person's permissions.

2. Holiday schedule configuration of persons' permissions:`[GET/PUT] /ISAPI/AccessControl/UserRightHolidayPlanCfg/<holidayPlanID>?format=json`.

3. Configuring holiday schedule of persons' access permission control for the device is not supported.