nurit

用于多重认证，加强信息资产安全

BaroPAM解决方案简介

2023. 3.

… 内容 …

Ⅰ. **解**决**方案**简**介**

Ⅱ. 认证**政策**

Ⅲ. **BaroBLE**

Ⅳ. **BaroCARD**

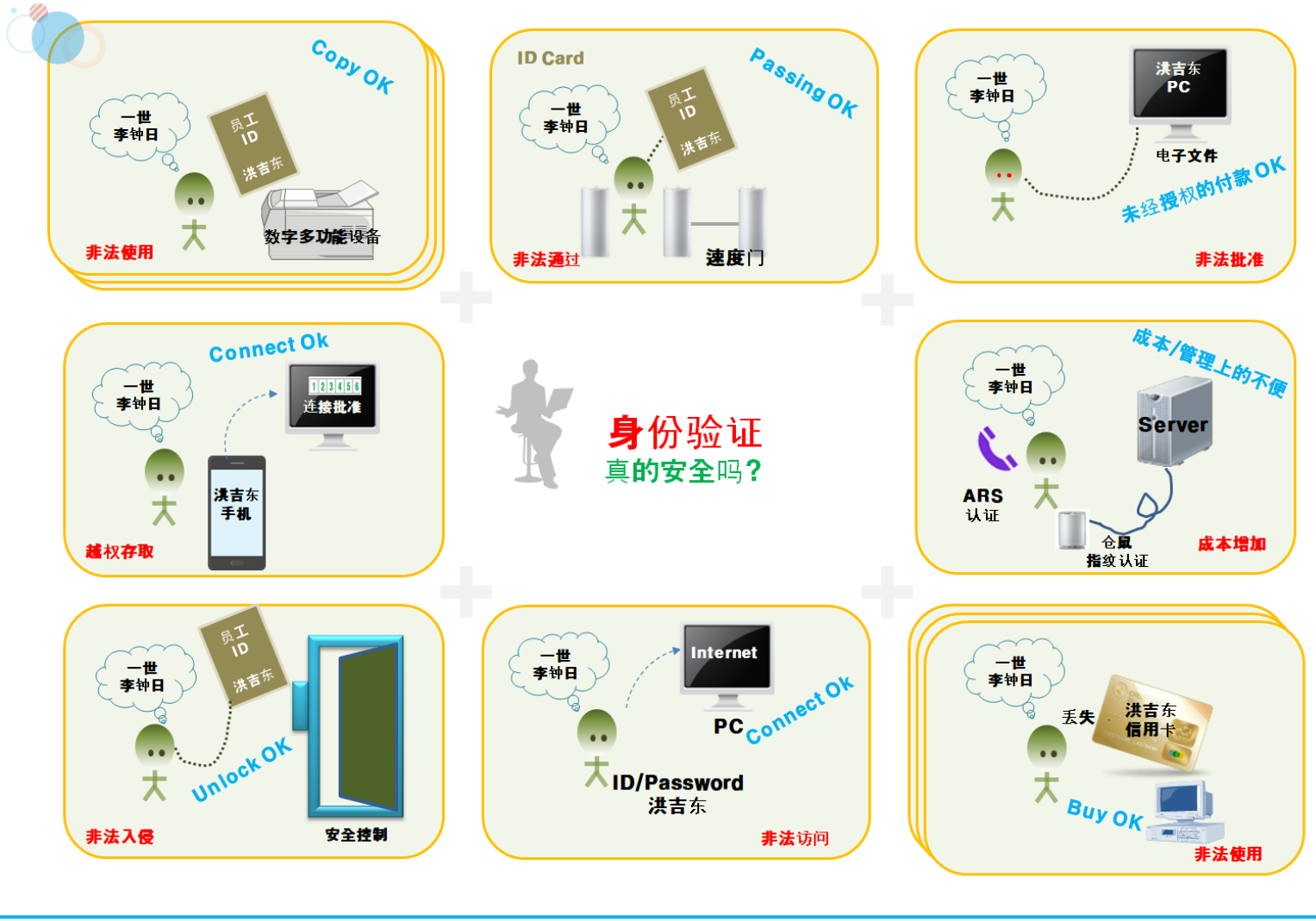
Ⅴ. **使用**与应**用**

Ⅵ. **等等**

nurit

Ⅰ. 解决方案简介

1. 身份验证的当前地址



nurit

2. 自我认证方法

包含个人信息的自我身份验证方法可以分为四大类：IP访问限制，公共证书，OTP(One-Time Authentication)和生物识别.

IP访问限制

IP访问限制方法要求信息资产（Windows，MacOS，Linux，Unix，数据库，网络设备，安全设备，存储设备等）使用固定IP，因此，如果您使用具有可变IP的动态IP，则访问限制是没有意义的.

认可证书

认证证书的方法使用成本高昂，并且由于认证证书认证模块的不便而难以使用，由于废除了强制认证证书，因此需要一种替代方法.

OTP

OTP方法对任何人都易于使用，不受时间和地点的限制，并且是一种简单的身份验证方法，因为OTP是从用户拥有的智能手机生成的，并且一旦使用就无法重复使用 °提供针对黑客攻击的强大安全性.

生物识别

这些天来备受关注的生物识别技术提供了强大的安全性，因为它们通过利用每个人的身体特征对每个人都是唯一的，但是解决方案的成本昂贵 °这几乎是不可能的 °因此，在最坏的情况下，可能会导致永久性损坏.

nurit

3. OTP分类和特征

OTP分为需要单独的身份验证服务器的硬件类型OTP和由于没有单独的身份验证服务器而不需要管理的软件类型OTP，可以轻松应用.

第一代OTP	第二代OTP
❖ 身份验证服务器方法（SHA-I），集成身份验证	❖ 模块认证方式（SHA-II），分布式认证
❖ 令牌，面向卡（OTP生成器）	❖ 面向智能手机（OTP生成器）
❖ 单独的Hmac Key发行和管理	❖ 单个Hmac Key不发行和管理
❖ 静态HMac Key方法	❖ 动态HMac Key方法
❖ 应用批量OTP生成周期（30 `60秒）	❖ 应用了单独的OTP生成周期（3~60秒）
❖ 非永久使用 / 产生的额外费用	❖ 永久使用 / 降低成本
❖ 二级身份验证（附加身份验证）	❖ 二级身份验证（附加身份验证）
❖ 价格昂贵 `应用受限 `管理复杂 `运营成本增加	❖ 成本低，应用范围广，管理简单，降低运营成本
❖ 需要用户信息同步	❖ 无需用户信息同步
❖ 身份验证拥塞时身份验证速度降低	❖ 认证拥塞时通过负载分配保证响应速度
❖ 通信和认证服务器故障时的服务中断（容易发生故障）	❖ 通信和认证服务器故障时灵活响应（服务有保障）

nurit

4.基本前提

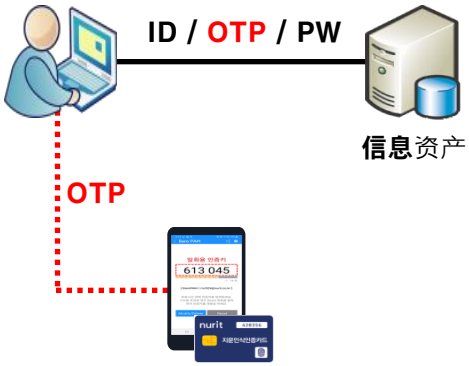
有没有一种低成本 `高效率 `安全性强 `简单 `不需要管理 `不需要任何障碍 `任何人都可以轻松应用和使用 `不需要额外引入单独的服务器或引入解决方案时的数据库？

你为什么需要这个？

5. 什么是BaroPAM？

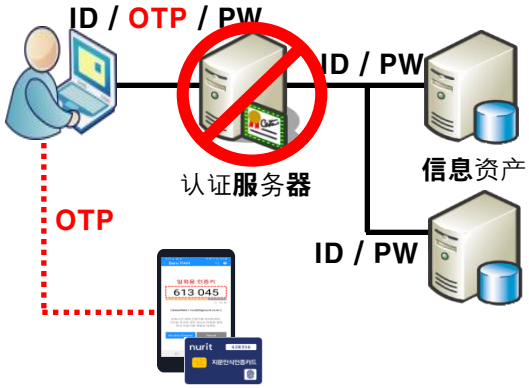
BaroPAM 解决方案是一种基于可插拔身份验证模块（PAM，Pluggable Authentication Module）方法的安全优化解决方案，任何人都可以轻松直接地应用于各种需要自我身份验证的操作系统和应用程序，以加强信息资产的安全性.

加强获取信息资产的安全性



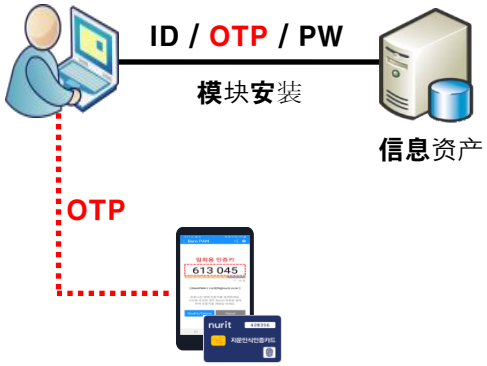
- 通过限制外部黑客或内部用户非法访问信息资产的情况来增强信息资产的安全性
- 一种将其他要素拥有的认证要素添加到ID / PW认证的认证技术，它是现有的具有两要素认证的“基于知识的认证”

维修方便



- 使用 BaroPAM 应用程序轻松进行身份验证，无需单独的身份验证密钥令牌/卡进行二次身份验证
- 单独的身份验证服务器不需要服务器来管理Windows / 服务器访问控制，从而降低了管理/运营成本

容易申请



- 通过在每个Windows或服务器上安装模块来简化应用程序
- 由于未重启Windows或服务器，因此即使在操作期间也可以应用
- 无需更改现有网络设备的设置

nurit

6. 解决方案功能

BaroPAM解决方案是模块认证方式的多认证解决方案，不需要单独的认证服务器. 安全性强，简单，无需管理，没有障碍，任何人都可以轻松申请并立即使用. 在引入解决方案时，它是一种低成本 `高效率的解决方案，不需要额外引入，例如单独的服务器或数据库.

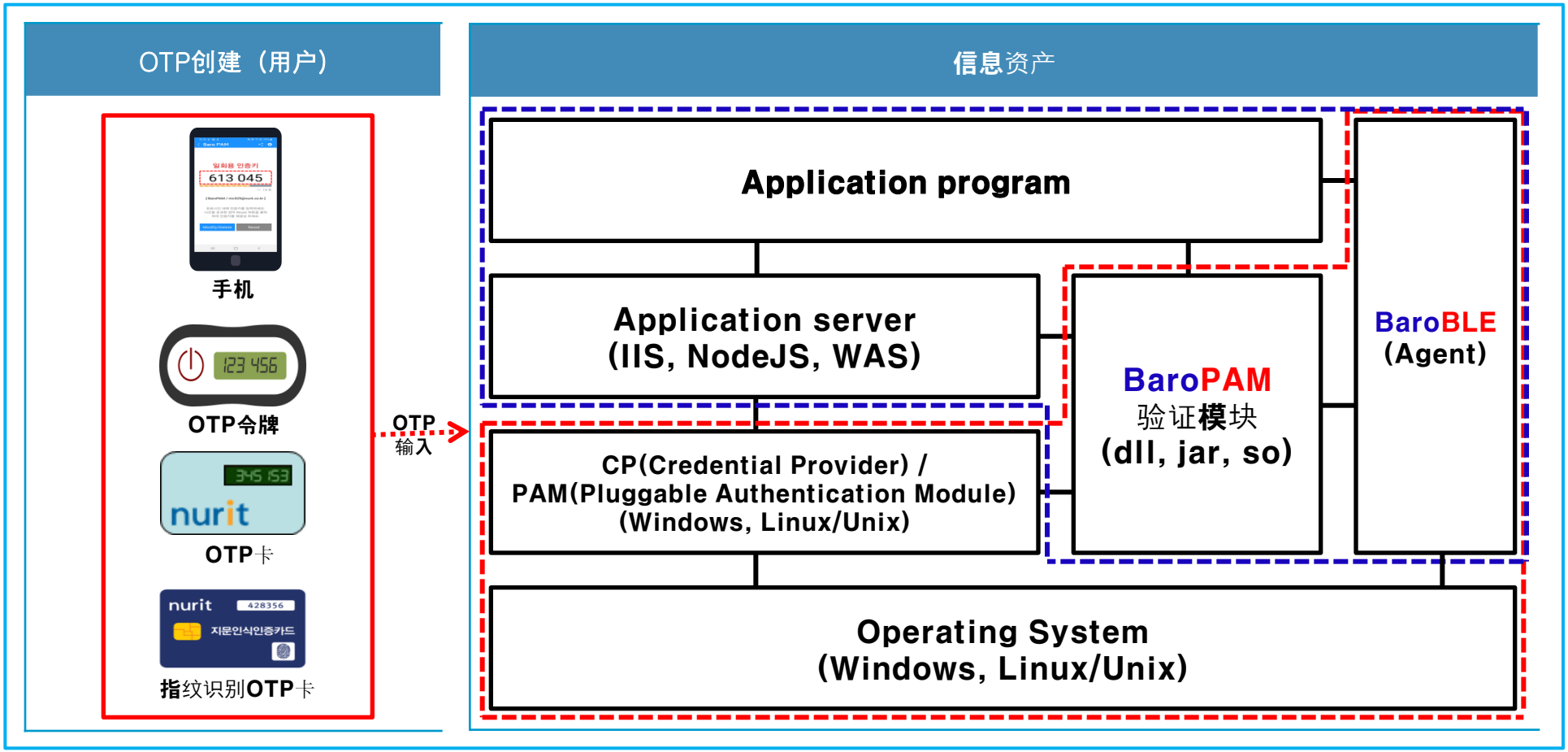
- 支持模块认证方式的二次认证，不需要单独的认证服务器
  认证速度快，服务有保障（平均认证时间0.01秒）
- 使用享誉全球的512Bit标准哈希函数
  （HMac-SHA512 /互联网安全标准IETF RFC 6238）
- 与硬OTP不同，软OTP允许永久使用
  即使在经常出现通信故障或安全的地区也可以进行认证
- 金融监督服务推荐的时间同步动态HMac密钥方法
  动态安全性，例如一次性或易失性，每次都发生变化或被使用和丢弃
- 使用智能手机等作为生成认证密钥的媒介，非常方便
  提供 App Lock On/Off 功能，为智能手机丢失时身份验证信息的暴露做准备
  iOS 提供了允许自我认证的功能
- 可以用于所有需要用户认证的领域，例如信息资产
  (信息资产的RADIUS身份验证期间还支持PAM/SQL身份验证)
- Windows 或 Open OS 的自动登录和屏幕保护程序 提供防锁/自动锁/自动释放功能
- 提供设置认证次数和时间限制的功能(例如30秒3次)
  提供防止中间人攻击的能力
  为可以被二级身份验证允许 / 禁止的帐户提供ACL功能
- 提供 BaroPAM 应用程序源混淆和屏幕捕获保护
  通过信息资产/帐户分别分配OTP和创建周期
- 提供免费的自定义和与各种应用程序的互锁开发
  （API与Java，C, C++等互通）

※ **HMac (Hash-based Message Authentication Code)：基于哈希的消息认证代码**

HMac是组合密钥以获得哈希函数的方法，并且是通过混合仅由发送方和接收方共享的消息和密钥来创建哈希值的方法.它还可以用于检查通过通道发送的消息是否已损坏. 由于Mac的特性，无法进行逆计算，因此将重新计算接收到的消息和哈希值，以检查计算出的HMac和发送的HMac是否匹配.

7. 溶液组成

BaroPAM 解决方案由用户生成一次性认证密钥的设备 `应用一次性认证密钥的信息资产 `验证一次性认证密钥的模块以及与 BaroPAM 应用程序通信的 BaroBLE 组成通过蓝牙



8.支持环境

BaroPAM解决方案支持OS `语言 `应用 `数据库 `网络设备 `ARM系统等各种需要二次认证（附加认证）的开发和运行环境，任何人都可以轻松应用.

No	구분		내용	비고
1	OS	Windows 系列	Windows 7或更高版本 2008 R2（NT 6.1）或更高版本	
		Linux 系列	Open Linux支持，例如Radhat，CentOS，AlmaLinux，debian，Fedora，Mint，Ubutu，openSuse，KaliLinux和Open OS(HamoniKR OS，Gooroom OS，TmaxOS) 等	
		Unix 系列	AIX, HP-UX, Solaris, FreeBSD, MacOS 等	
2	Language		C, C++, C#, Java 等	
3	Application	ARM system	提供分片对象（身份验证，加密/解密）	
		IIS	提供dll（身份验证，加密/解密）	
		NodeJS	提供jar（身份验证）	
		WAS	提供jar（身份验证，加密/解密）	
4	Database	加密与解密	Oracle，Tibero，MySQL，MariaDB，PostgreSQL等	
		验证	支持Radius身份验证的数据库，例如Oracle，MySQL，MariaDB，PostgreSQL等.	
5	Network设备		支持Open Linux和Radius身份验证的设备	

9.需要介绍

"如果信息资产的登录ID /密码泄露，还有其他选择吗？"

1. 为了增强安全性，应用两步式身份验证系统使用OTP进行用户识别和身份验证

未指定辅助身份验证(例如ID / PW + OTP)的应用，在身份验证失败超过特定次数(例如5次或更多) 时阻止访问的方法，但是在基于知识，基于所有权和基于特定对象之间有所不同认证方法：必须同时使用属于该方法的两种认证方 式.

2. 通过恶意代码阻止非法远程访问，恶意代码是为恶意目的而创建的程序

通过恶意代码程序非法获取信息资产(从桌面到应用程序，从桌面到桌面，从桌面到服务器，从桌面到数据库，从服务器到服务器等)的信息资产的访问信息之后，该程序是为恶意目的而创建的程序，远程非法访问信息资产. 您应该阻止访问.

3. 由于丢失，被盗或被黑客入侵而用于重置用户密码

自行登录-输入ID，特定项目和一次性身份验证密钥以注册并使用新密码(如果正确).

4. 通过与其他产品区分开来的战略来领导市场，作为销售增长的催化剂

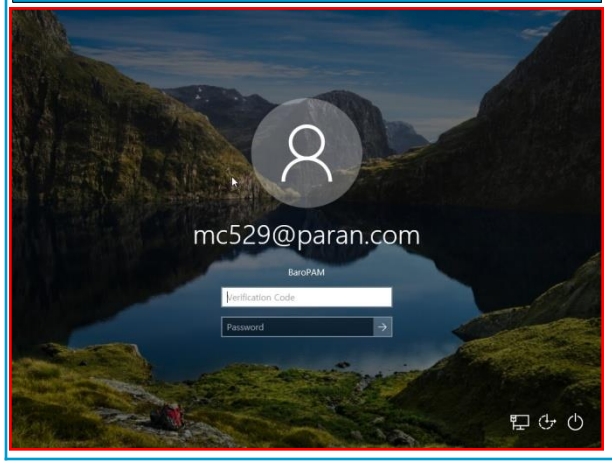
俗话说："如果什么都不做，中间就走"，这在云时代是行不通的. 在新时代，一种新的防护装置适用. 使用单个密码保护门是一种较旧的方法. 系统和基础架构一直在不断变化，以适应新的系统和基础架构，现在是时候让每个人自己检查为什么它们坚持旧的了.

10. 申请方案

登录信息资产时，永远不会单独使用密码来保证安全，因此需要一种新的应用程序方法（附加身份验证，密码替换，新密码），该方法可以在每次使用时替换或附加身份验证（辅助身份验证）.

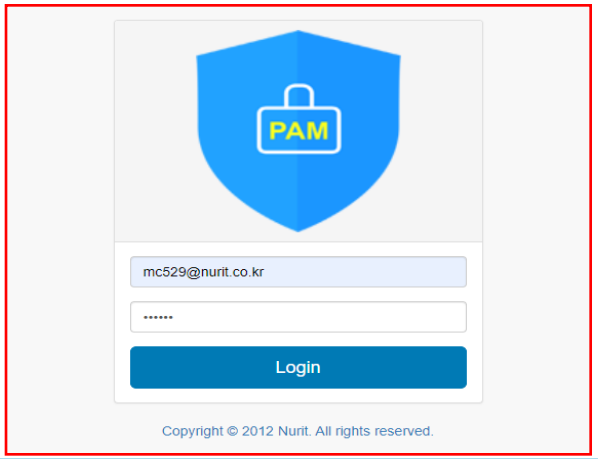
1个计划（附加证明）

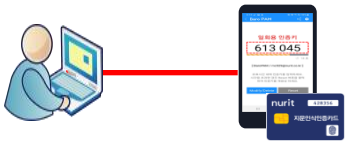
使用登录名和密码以外的其他身份验证（辅助身份验证）应用OTP
(ID/PW/OTP)



2计划（密码替换）

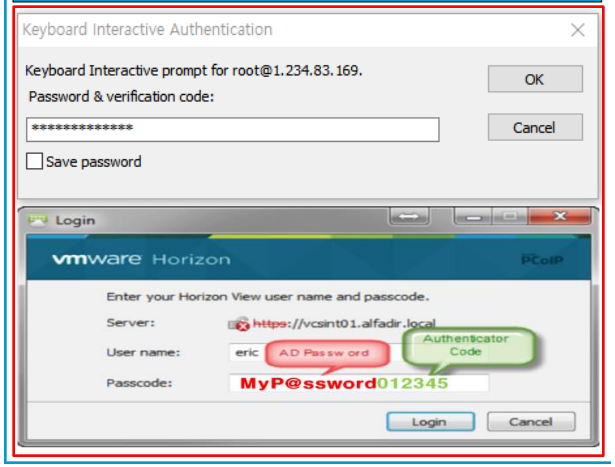
删除密码 替换为OTP
(ID/OTP)





3计划（新密码）

通过组合密码和OTP，将创建一个新的一次性密码，并将其应用于每个OTP生成周期
(ID/PW+OTP)



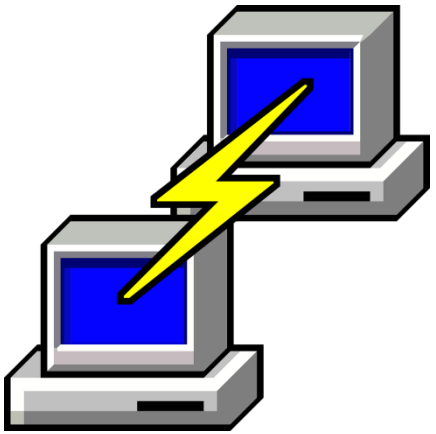
nurit

11. 增强安全性

通过结合检测和删除恶意代码的疫苗解决方案 `为恶意目的创建的程序以及通过对信息资产的访问控制进行二次认证来阻止帐户盗窃 `权限提升和非法绕过/远程访问的 BaroPAM 解决方案，信息资产的安全性可以产生协同效应，加强。

信息资产安全 = **恶意软件检测 / 清除 (疫苗)** + **阻止远程访问 (BaroPAM)**

- Windows NT Server
- Mac OS
- Linux / Unix Server
- Application
- Database
- Network, IoT Device
- 저장장치



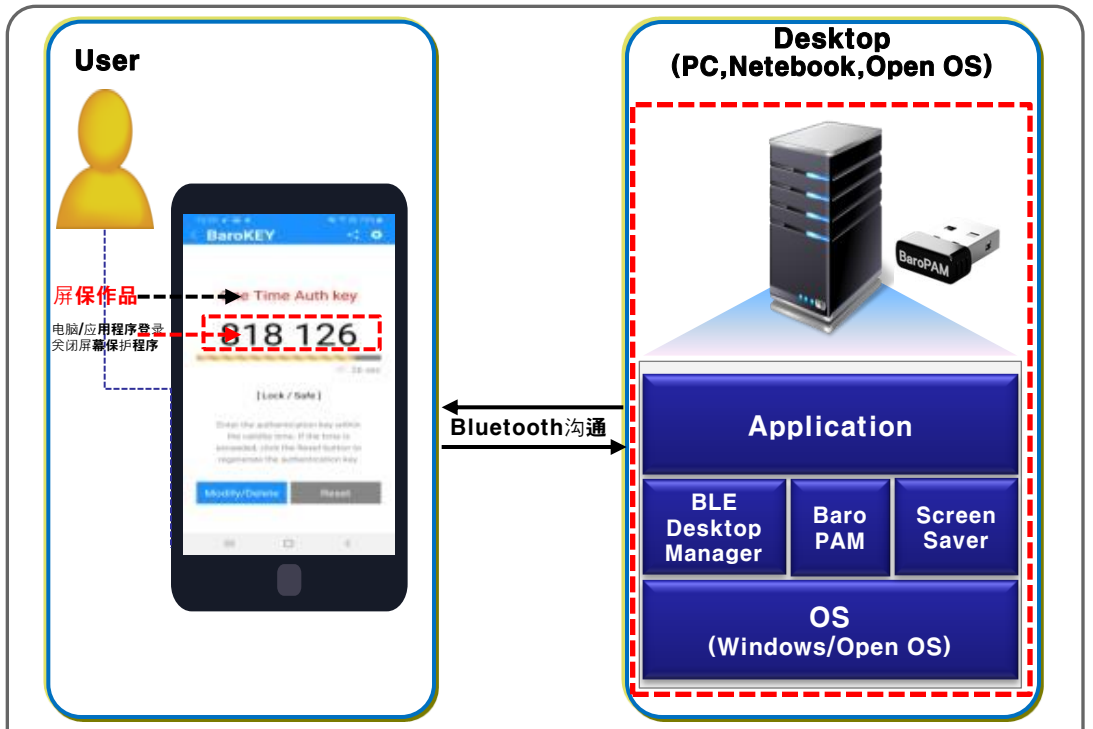
Desktop to Application
Desktop to Desktop
Desktop to Server
Desktop to Database
Server to Server

1. 认证政策

BaroPAM解决方案对所有信息资产的认证策略不是针对各种攻击的综合保护方法，而是对每个组件逐一保护的方法，您可以安全地保护您的信息资产.

1.什么是 BaroBLE?

BaroPAM解决方案的BaroBLE是Windows或打开的操作系统(HamoniKR OS, Gooroom OS, TMaxOS)的自动登录和屏幕保护的防锁定/自动锁定/自动解锁功能 °为了信息安全，屏幕阻塞5分钟，屏幕保护10分钟，强制设置终端安全和省电功能，如将关机时间设置为 4 小时，以增强信息安全并最大限度地减少用户的不便.



① 如果您单击韩文名称"One Time Auth key"，连接到 BLE (1:N) 的屏幕保护程序将起作用.
(即使智能手机和终端在一定距离之外，BLE 连接(1:N)的屏幕保护程序也能工作)
② 如果点击生成的认证信息 "818 126"号，则显示与取消BLE连接(1:N)屏保并点击"Reset"按钮相同的认证密钥.

需要 BaroPAM 屏幕保护程序

如果你**看最近的安全事件，大部分都是因**为违**反**内**部安全**规**定而**导**致的**问题.

不使用屏**幕保**护**程序和密**码 `违**反或疏忽安全**规**定 `感染**恶**意代**码 `离开个**人**终端时使用**远**程**桌**面等都可能**导**致安全**问题.

因此，为**了**个**人**电脑**的信息安全，**终**端安全和省**电**同**时实现，设**置**屏**幕**屏蔽5分**钟，屏**幕保**护**10分**钟，**强制**关**机4小**时.

屏**保有**时会导**致用**户**坐着**时**无法使用**电脑，**此**时屏**保自**动启动，给**用**户带来**不便.

nurit

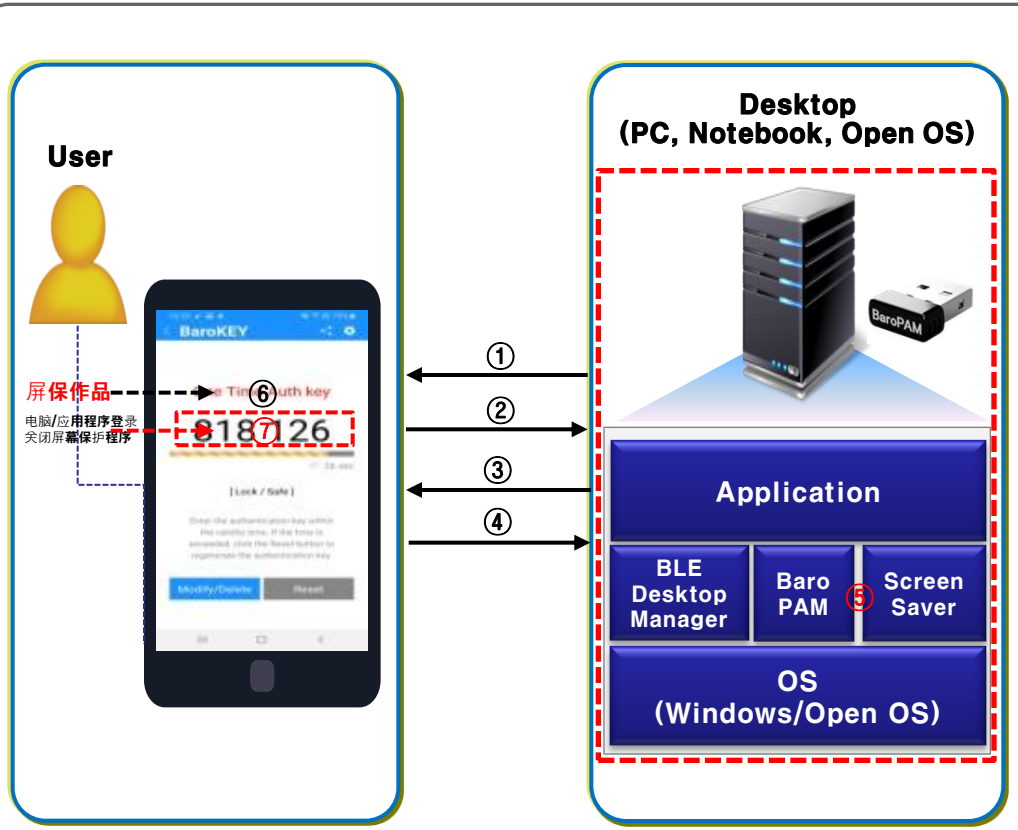
2. BLE USB 加密狗(BlueIO)

BleuIO 是一款低功耗蓝牙 (BLE) USB 加密狗，是一款低功耗蓝牙 USB 加密狗，可用于以最快 `最简单的方式创建新的 BLE 5.0 应用程序 °适用于 Windows 或打开的操作系统的自动登录和屏幕保护锁定/锁定保护. /用于自动释放功能，负责BaroPAM app与桌面的通讯.

分配	解释
角色	可编程蓝牙中央或外围设备. USB 设备.
安全	具有 ECC, AES-256, SHA-1, SHA-256, SHA-512 和随机数生成器的加密引擎.
连接	蓝牙 5.0 和 USB 全速
力量	**USB +5V**
芯片	**DA14683**
记忆	闪存 8Mbit & OTP 64KB
尺寸	**19.2mm(L) X 16.3mm(W) X 6.2mm(D)**
温度	**-20 ~ +65C**
案例材料	PBT + 20% 玻璃纤维
认证	**CE, FCC, KC, RoHS, REACH等**
颜色	白色（用于 HID）/黑色（用于 CDC）
支持环境	**Windows 10, MacOS, Linux**
其他	制造商：瑞典智能传感器设备 原产地：马来西亚

3.架构和身份验证过程(登录和屏幕保护程序)

BaroPAM 解决方案的 BaroBLE 增强了 Windows 或开放式操作系统(HamoniKR OS, Gooroom OS, TMaxOS)的信息安全性，并最大限度地减少了用户的不便，同时防止了 Windows 或开放式操作系统的自动登录和屏幕保护锁定/自动锁定/自动发布的架构和身份验证程序如下面所述.



* BLE：Bluetooth Low Energy,低功耗蓝牙

认证处理流程

① 在桌面上搜索使用 BaroPAM 应用程序设置的蓝牙频道.
② 如果蓝牙通道设置在 3~6M 范围内，BaroPAM app会响应.
③ 如果桌面自动登录或屏幕被锁定,则需要从 BaroPAM应用程序请求一次性验证密钥.
当桌面屏幕处于活动状态时,屏幕不会锁定,直到与 BaroPAM应用程序的连接断开.
④ 在 BaroPAM 应用程序中创建一次性认证密钥后,用桌面响应一次性认证密钥.
⑤ 确认一次性认证密钥的有效性后，桌面解锁屏幕.
⑥ 屏保操作：点击英文"One Time Auth key",开启BLE (1:N) 连接的屏保. 即使 BaroPAM 应用程　序与桌面有一定距离,通过BLE(1:N)连接的 屏幕保护程序也会被激活.
⑦ 屏保释放：点击"818 126"数字,即生成的一次性认证密钥, 重新生成一次性认证密钥,方式与取消BLE连接的屏保相同 (1:N) 并单击"Reset"按钮.

nurit

1.指纹OTP卡

BaroCARD解决方案是应用指纹信息即生物特征信息的最优自我认证解决方案，在塑料卡上注册指纹信息即生物特征信息，并识别注册的指纹信息后，卡片生成一次性认证密钥（具有内置指纹识别功能和认证卡，是一种新概念卡），被称为指纹识别OTP卡.

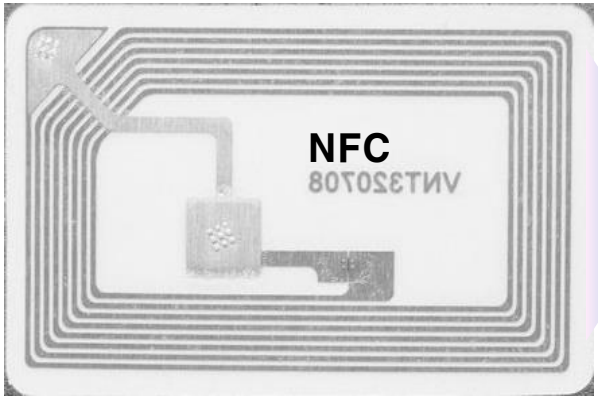
✓指纹信息登记装置	No
✓指纹信息识别装置	No
✓保存指纹信息服务器	No
✓指纹信息泄漏事故	No
✓非法使用指纹卡	No

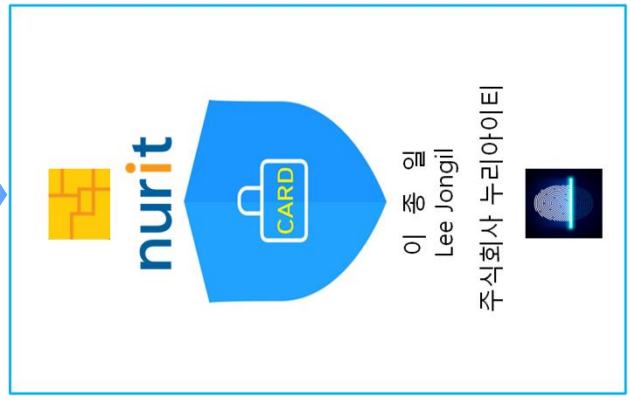
※员工身份证/身份证/访问/安全/Lock/OTP/支票卡/信用卡/交通卡

nurit

2.指纹识别安全/门禁卡

BaroCARD解决方案是一种应用生物指纹信息的最佳自我认证解决方案，在塑料卡上注册生物指纹信息并识别出注册的指纹信息后，该卡会**生成一次性身份验证密钥（内置指纹识别功能和身份验证卡）一种新概念卡），称为指纹识别OTP卡.**





✓指纹信息登记装置	No
✓指纹信息识别装置	No
✓保存指纹信息服务器	No
✓指纹信息泄漏事故	No
✓指纹信息泄漏事故	No
✓使用指纹卡充电	No

※员工身份证/身份证/访问/安全/Lock/支票卡/信用卡/交通卡

nurit

3. BaroCARD组成

BaroCARD解决方案包括充电式指纹识别，指纹识别+ OTP，以及使用从电子设备产生的感应电流的非充电方法.

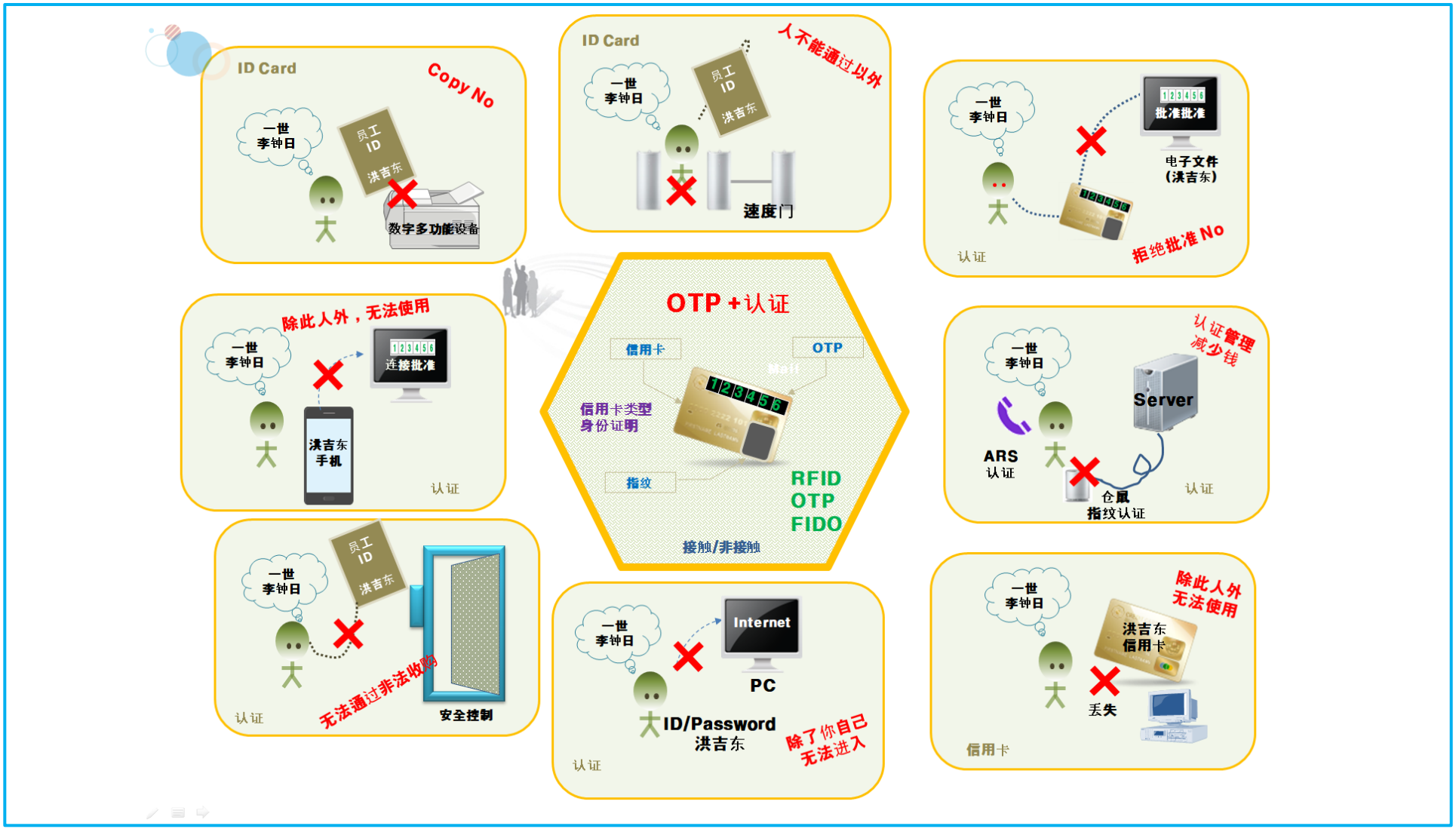
项目	指纹识别	指纹识别 + OTP	No Battery
MCU工作温度 指纹传感器工作温度 电池工作温度（二次电池） 功率	-40℃ to +85℃ -40℃ to +85℃ -20℃ to +60℃ 3.3V	-40℃ to +85℃ -40℃ to +85℃ -20℃ to +60℃ 3.3V	-40℃ to +85℃ -40℃ to +85℃ - 3.3V
运行期间的电流消耗 待机电流消耗 EER	6mah - < 0.04%	6mah 1uah < 0.04%	6mah - < 0.04%
Enrollment time Verification time 指纹注册	0.5sec 0.5sec 20	0.5sec 0.5sec 20	0.5sec 0.5sec 20
Sensor type Sensing area Size sensing array Pixel resolution	Touch area sensor 8.00 x 8.00 x 0.65 mm 160 x 160 Pixel (508dpi) 256 gray scale values	Touch area sensor 8.00 x 8.00 x 0.65 mm 160 x 160 Pixel (508dpi) 256 gray scale values	Touch area sensor 8.00 x 8.00 x 0.65 mm 160 x 160 Pixel (508dpi) 256 gray scale values
应用领域	员工身份证/身份证 访问/安全/Lock 支票卡 信用卡 交通卡	员工身份证/身份证 访问/安全/Lock OTP 支票卡 信用卡 交通卡	员工身份证/身份证 访问/安全/Lock 支票卡 信用卡 交通卡

指纹OTP充电和待机时间（基于20mah电池）：1小时内
电池使用时间为睡眠：8年（基于当前消耗的220nah），
Active: 4个月=>指纹3秒（基于电流消耗7mah），OTP时间30秒（基于电流消耗550uah）

nurit

Ⅴ. 使用与应用

1. 可用面积



nurit

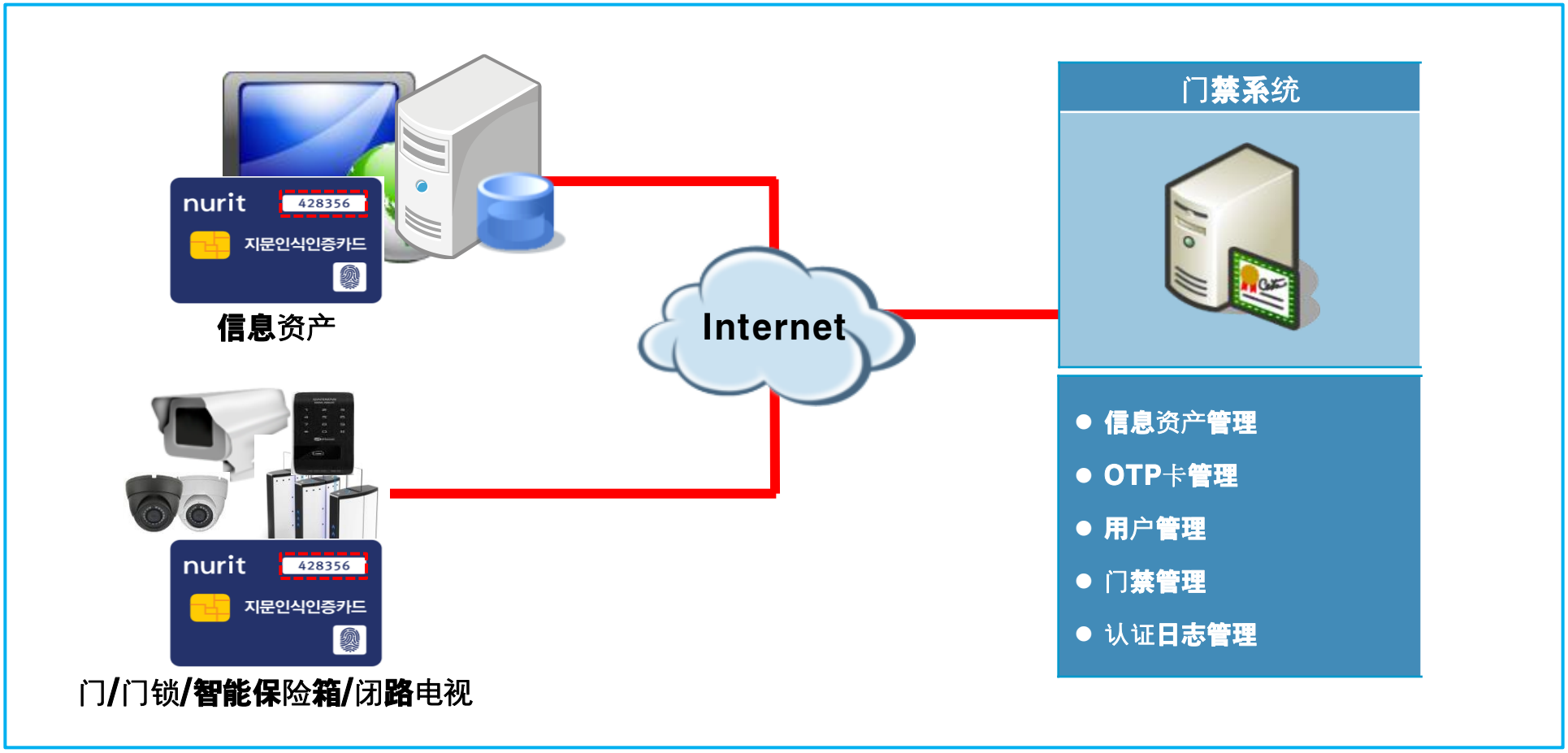
2. VDI / SSO /移动虚拟化平台/ 5G无线AP / VPN / SAC身份验证

BaroPAM用于用户识别和身份验证，以增强IoT设备/ VDI / SSO /移动虚拟化平台/ 5G无线AP / VPN / SAC等解决方案的安全性.

OTP申请之前	OTP申请后
❖ 对每个信息资产 / 帐户使用固定密码	❖ 信息资产/帐户对OTP的使用
❖ 应用密码生成规则	❖ 应用哈希算法生成的值（ SHA512 ）
❖ 将密码信息存储在数据库中	❖ 如有必要，直接从智能手机应用程序创建
❖ 需要使用加密技术等的安全措施（ 单向加密	❖ 使用加密技术等无需采取任何安全措施
❖ 泄漏和损坏的风险	❖ 无溢出危险，无损坏
❖ 强制密码更改周期	❖ 应用了单独的OTP生成周期（ 3~60秒 ）
❖ 密码综合症 / 密码重置综合症投诉	❖ 无密码综合症/密码重置综合症

3. 信息资产和门/门锁/智能保险箱/闭路电视的集成认证

这是一种集成式身份验证，将OTP与单个（指纹身份验证）身份验证卡一起用于用户标识和身份验证，以增强信息资产登录和门/门锁/智能保险箱/ CCTV的安全性.



nurit

4. 集成的门锁/智能保险箱认证（通行管理/一次性）

BaroPAM验证模块安装在门锁/智能保险箱中，以增强OTP的安全性和便利性.

* OTP: One-Time Password

预期效果：安全/便利性增强

- 无需记住设置的密码，使用OTP创建APP输入密码
- BaroPAM验证模块直接移植到门锁/智能保险箱，因此不需要单独的身份验证服务器
  - 初始服务器/网络设备投资成本降低
  - 即使在服务器之间的通信失败的情况下也可以使用服务
- 可与智能手机APP集成

- 带指纹认证的OTP输入OTP卡与OTP卡和指纹识别模块结合使用
- 个人指纹信息存储在指纹识别模块中的卡本身上
  - 简单的指纹输入程序
  - 最大限度地降低入侵生物特征（指纹）信息的风险
  - 安全，因为当丢失卡时它是一种指纹识别方法
- 可以集成防御，信用卡/借记卡，员工ID /护照/安全卡等

5. CCTV综合认证（通行证管理/一次性）

BaroPAM被用于用户识别**和**认证，**以符合《信息和通信**网络**法》和《个人信息保**护**法》**，**并**通**过一种经过验证**的解决**方案增强CCTV解**决**方案的安全性，**并**安全，方便地**对**其**进**行管理.**

* OTP: One-Time Password

问题 / 改进

- **指**导**更改公共机**构闭**路**电视**管理机**构**的密**码
  - 对**于CCTV**产**品**，**请**使**用默**认**密**码
  - **通**过**Internet**轻**松**访问**CCTV**，**允**许访问内**部**网络
- 闭**路**电视**控制中心**拥**有**数**百或**数**千**个闭**路**电视
  - 将**存**储**的CCTV**图**像委托**给**私人公司**
  - **无法手**动**管理大量CCTV**（**一次性身**份验证）
- **需要遵守**《个**人**视频**信息保**护**法》**并应对审**核**
- **通**过辅**助身**份验证（**附加身**份验证）**保**护**CCTV的信息**资产
- **通**过将**密**码**替**换为**一次性身**份验证**密**钥来**防止非法使用**
- 视频**信息保**护**措施的建立和**运**行**
- 备份视频**信息**时应**用加密/解密**
- **通**过对**IP**摄**像机**应**用**辅**助身**份验证（**附加身**份验证）来**增强安全性**

nurit

VI. 等等

1. 软件质量认证（GS证书/测试报告/专利证书/版权注册证书）

2017年七月
GS认证1级

2017年七月
TTA测试报告

2014年6月
专利号
10-1413971号

2022年6月
软件互操作性测试

2019年3月
著作权登记证

2. BaroSolution系列

系列	说明	备注
BaroPAM	一个简单而强大的信息资产访问控制身份验证解决方案，通过将OTP与辅助身份验证集成在各种信息资产的操作系统和应用程序中，支持集中式身份验证机制.	
BaroCARD	指纹识别OTP卡解决方案，该卡解决方案是在将生物特征指纹信息注册到塑料卡上之后识别注册的指纹信息时生成OTP的卡.	
BaroCRYPT	一种基于XXTEA（Extended Extended Tiny Encryption Algorithm）的轻量级，最快的加密算法， 这是一种块加密算法，体积小巧，易于使用Feistel密码实现.	
BaroCollector	具有分布式处理，可靠性和可用性的实时日志收集器，可将各种来源生成的大量日志数据（大数据）有效地收集到中央数据存储中.	
BaroFDS	它是金融部门中唯一经过验证的FDS解决方案，其解决方案是基于母公司金融机构在检测和应对异常金融交易方面的2年专业知识而开发的，可以轻松，快速地在复杂的金融环境中应用，并在施工后立即生效.	
BaroIDS	通过基于现场专业知识的FDS（欺诈检测系统）开发的解决方案，用于检测和阻止对信息资产（服务器，网络设备，安全设备，存储设备，数据库，应用程序等）的异常访问.	

nurit

您无需记住密码!
BaroPAM与您同在.

谢谢!

www.nurit.co.kr
mc529@nurit.co.kr