Indeed Card Management
Smart card lifecycle management system

Introduction
User digital signature, strong authentication and data encryption have become quite common for most of the modern companies. These technologies require employees to have personal secure devices: USB tokens or smart cards, giving start to a whole new specter of management and usage control tasks. Indeed Card Management (Indeed CM) allows to take on these challenges and gain the following benefits:

● effectively manage smart card life cycle
● keep logs and audit administrator and user actions
● automate user certificate management processes
● backup key information
● provide users with mechanisms of self service to easily perform smart card usage related tasks

The document contains description of basic operation principles and Indeed CM architecture.

Prerequisites for Smart card lifecycle management systems introduction
Public Key Infrastructure (PKI) usage is connected with a lot of routine operations for issuing, management and revocation of certificates and smart cards. Certification Authority base tools are not designed for the users' smart cards management and provide only the basic operations with certificates. The necessity in the specialized tools for smart cards and certificates management arises in the following cases:

● Users certificates are applied to the business critical operations
  In this case the full usage of the smart card abilities as the secure information storage is necessary. The efficient management and control of smart cards usage is required.

● A company uses more than one certificate for the user
  IT services work for support of PKI integrity state is increasing when increasing the number of certificates.

● Remote smart cards usage
  The ability of secure smart card unblocking not discreditable the administrator PIN code is necessary if the smart card is blocked in the remote mode.

● Creating an integrated access management system on the basis of certificates and smart
Modern smart cards are suitable to use outside the PKI. One of the examples is employing the hybrid RFID smart cards to physical access in Access Control Systems (ACS), usage Single Sign-On systems, etc.

List of terms and definitions

**Smart card, USB token** – user's personal secure device, which holds user's key data. It could be in form the smart card or USB token. Usually key data consists of personal digital certificate and private encryption key.

**Open key certificate (certificate)** – digital document which verifies correspondence between public key and key user's identification data. Contains user data, purpose and sphere of public key application, certification center’s name, etc.

**Asymmetric encryption algorithms** – encryption algorithms which employ different keys for direct and backward transformation.

**Public key** – key couple component employed in asymmetric encryption algorithms. Public key is protected from forgery and published for usage by all cryptographic operations participants. Data encryption and digital signature verification is completed by means of a public key.

**Private key** – secret key couple component employed in asymmetric encryption algorithms. Comparing to the public key, private key is stored in secret in a secure segment of smart card memory. Private key is used to evaluate digital signature and decryption.

**Certification Authority (CA)** – an entity that issues digital certificates. CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

**Public key infrastructure (PKI)** – a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

**Digital signature (DS)** – requisite of a digital document which allows to avoid falsification of data in a digital document from the moment of digital signature creation and verify the affiliation of the signature to the certificate's owner. Can be a full analog to a personal signature in cases described for by statute or law.


**Indeed CM architecture**

Indeed CM architecture scheme is bellow.
Indeed CM consists of the following components:

- **Indeed CM Server**
- **Indeed CM Event Log**
- **Indeed CM Connectors**
- **Indeed CM Database**
- **Indeed CM Runtime Environment**
- **Indeed CM Credential Provider**

**Indeed CM Server** – main component of Indeed CM infrastructure. Web application that operates on a server Internet Information Services (IIS). Indeed CM Web Application provides centralized system user, card repository and security policy management. Besides that, Indeed CM Web Application processes smart card unblocking and logging operations.

**Indeed CM Event Log** – event log for Indeed CM. Event log records all events connected with smart card lifecycle and alteration of system parameters. Log view is available in Indeed CM Web Application interface, which also allows to create reports according to various criteria.

**Indeed CM Connectors** – Indeed CM adapter module library for external systems. These modules allow to react on events that arise in Indeed CM and take additional actions. As an example of Indeed CM Connector realization we can suggest integration with Certification Authority, which allows to automate user certificate management (issue, revoke, suspend).

**Indeed CM Database** – data storage for Indeed CM. Data can be stored in database management system (DBMS) or Active Directory. When storing data in AD, no schema extension is required. All data is localized in a separate container.

**Indeed CM Runtime Environment (Indeed CM RTE)** – client software installed on administrator and
user workstations. Indeed CM RTE allows to perform operations that require a smart card access: a new card registration, issuing a new card, certificate enrollment, etc.

Indeed CM Credential Provider – client module which allows to unblock the blocked smart card at the user's workstation online and offline without OS authentication.

Communication between Indeed CM components is established by means of the following protocols:
- ADSI (Active Directory Service Interfaces) – for operation with Active Directory.
- Encrypted RPC – for Indeed CM connection with Certificate Authority for operation with user certificates.
- HTTPS (using SSL) – for accessing Indeed CM Web Application.

Smart card lifecycle

Given diagram illustrates a smart card lifecycle in Indeed CM system. The smart card exists in one of the following states:

- **Unregistered** – The smart card is not registered in Indeed CM database.
- **Clean** – The smart card is registered in the system, but all data is deleted and card is programmed with administrator's PIN code.
- **Assigned** – The smart card is associated with a specified employee, but is not initialized with operation data.
- **Pending** – The system awaits verification of user's personal certificate from Certification Authority.
- **Issued/Enabled** – The smart card is initialized and has recorded data (user PIN code, PIN code policies, certificates), smart card backup is completed. Card is given to the employee for further use.
- **Disabled** – The smart card is temporarily disabled and unavailable for operations, user certificates are suspended (temporarily revoked).
- **Revoked** – The smart card is blocked and user certificates revoked. Revocation procedure is irreversible and card can not be activated after its completion.

Indeed CM scenarios

All Indeed CM system operation scenarios can be divided into three groups:
regular user operations
Indeed CM Help Desk operations
Indeed CM administrator operations

Regular user operations
Users can access various operations related to the lifecycle of their smart cards and USB tokens. Such operations are completed through the self service interface or PC interface (card unblocking scenario) and contain the following possible actions:

- Adding and issuing a card (Add, Issue). These operations are available if security policies have relevant user permissions.
- Blocking an active card (Disable)
- Activating a blocked card (Enable)
- Revoking a card (Revoke)
- Changing a smart card PIN code

Indeed CM Help Desk operations
The main task for Help Desk operators is user support. For completion of this task all operations connected with the user card lifecycle are available to them:

- Adding smart card (Add) into Indeed CM database
- Deleting smart card (Remove) from database
- Assigning smart card to a certain user (Assign)
- Issuing a card (Issue)
- Blocking/Activating a smart card (Disable/Enable)
- Revoking a card (Revoke)
- Cleaning a card (Clean)
- Temporary or permanent replacement of a smart card on a new one

All specified operations are completed in Indeed CM web interface.

Indeed CM administrator operations
Administrators have the most rights in Indeed CM. They have access to all Help Desk operators actions and also a set of additional Indeed CM policy management operations. Policies are the key object in configuring Indeed CM and contain various system parameters:

- Certification Authority connection settings
- certificate templates
- a smart card lifecycle settings
- a smart card PIN code policies
- key questions for user authentication (used in smart card unblocking scenarios)

System audit
Help Desk operators and Indeed CM administrators can view system log in the same web interface where they complete their tasks. At the same time they can compile reports using different event selection criteria: time period, a smart card type and serial number, operator's name, user's name, event type, etc.

User data protection
Indeed CM user data protection consists of two main elements:

- **In-storage data protection**
  Symmetric encryption algorithms and hashing, which are a part of Microsoft Enhanced Cryptographic Service Provider\(^1\), are employed for storage data protection. All encryption

\(^1\) By default AES and SHA algorithms are used. Upon necessity other algorithms and Cryptographic Service
operations processed within Indeed CM server, encryption keys do not leave the server.

- **CM Web Application - client communication line protection**
  For data protection in the communication line between Indeed CM web application and a client (web browser) SSL\(^2\) encryption protocol is used. This protocol is supported and implemented by the Internet Information Services web server and provides secure communication between client and server.

## Indeed CM Advantages

### Various smart card vendors support

Indeed CM is designed to operate with various smart cards, so all the supported cards can be used in one infrastructure. Solution's architecture allows to easily support new smart cards by implementing appropriate middleware. At the moment the following devices are supported:

- A virtual smart card Indeed AirKey Enterprise
- Rutoken USB tokens from Aktiv company
- eToken smart cards and USB tokens from SafeNet company
- ESMART smart cards and USB tokens from ISBC company
- AvestKey USB tokens from Avest company
- IDPrime smart cards from Gemalto company

### CryptoPro support

Indeed CM supports CryptoPro CA and also CryptoPro CSP. This allows to use Indeed CM inside infrastructures that require GOST (Russian federal standard) encryption.

### Simplicity of interaction between system and end-user

The state-of-the-art technologies and user tasks centered approach are used in Indeed CM development. This allows to provide all process participants with comfortable and effective interaction mechanism. Indeed CM Web Application has modern practical and functional user interface, which can be flexibly adapted to user's device. That is why system operation is equally comfortable when using it on personal computer, smartphone or tablet PC.

### Integration with Indeed AM

Indeed CM integration with Indeed AM logical access management system allows to link smart card and token lifecycle with user credentials lifecycle. At the moment of issue of the smart card, administrator can define user application access profile (Single Sign-On profile). So when the employee gets his secure device from the administrator, all necessary credentials are enrolled and accessible by means of the smart card. Indeed CM console is the only management point for devices, certificates and passwords lifecycles. Integration with Indeed AM simplifies providing and gaining network and application access.

### Licensing

Indeed CM employs CAL (client access license) license. This license grants the right to use Indeed Provider (CSP) realizations can be used.

\(^2\) [Secure Sockets Layer](https://en.wikipedia.org/wiki/Secure_Sockets_Layer)
CM product and register smart cards for one user. License is provided for a number of Indeed CM user accounts. Number and content of CAL license type can be increased by purchasing additional licenses. Amount of client software installations (workstations) is not limited.

Client Access License is "captured" for the specified user. Upon necessity licenses of the CAL type can be redistributed between employees (license can be revoked from one employee and assigned to another).

**System requirements**

**Network infrastructure:**
- Microsoft Active Directory 2003/2008/2008 R2 Domain (Native mode)
- Forest and domain functional levels: Windows Server 2003 and higher

**Indeed CM Web Application**
- Internet Information Services 7 и выше
- Windows Server 2008 Standard/Enterprise SP2 32/64bit
- Windows Server 2008 R2 Standard/Enterprise SP0/SP1

**Indeed CM Runtime Environment**
- Windows XP 32bit SP3 Windows XP 64bit SP2
- Windows Server 2003 Standard/Enterprise SP2 32/64bit
- Windows Server 2003 R2 Standard/Enterprise SP2 32/64bit
- Windows Vista SP2 32/64bit
- Windows 7 SP0/SP1 32/64bit
- Windows Server 2008 Standard/Enterprise SP2 32/64bit
- Windows Server 2008 R2 Standard/Enterprise SP0/SP1
- Internet Explorer 8 and higher (for operations that require a smart card connection to the PC)
- Additional requirements are specified by the system requirements of the selected smart card

**Indeed CM Credential Provider**
- Windows Vista SP2 32/64bit
- Windows 7 SP0/SP1 32/64bit
- Windows Server 2008 Standard/Enterprise SP2 32/64bit
- Windows Server 2008 R2 Standard/Enterprise SP0/SP1

---

**Full list of Indeed ID products**

| AirKey | **Indeed AirKey Cloud (Indeed AK Cloud)**
|        | The cloud platform supported digital signature, strong authentication and delivery of encrypted messages to the user’s smartphone.
|        | **Indeed AirKey Enterprise (Indeed AK Enterprise)**
|        | The software smart card supported any operations available for hardware-based keys.
| Card Management | **Indeed Card Management (Indeed CM)**
|                 | Smart cards and user certificates lifecycle management system.
| Enterprise Authentication | **Indeed Enterprise Authentication (Indeed EA)**
|                           | Active Directory users access to the company information resources using strong...
<table>
<thead>
<tr>
<th>Enterprise Single Sign-On</th>
<th>Indeed Enterprise SSO (Indeed ESSO)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strong authentication for the users access to the company information systems without necessity of modifying them.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indeed Rules System ACS Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with the physical access control systems that provides an additional factor of authentication (the employee's location on the premises) to information systems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indeed ESSO IdM Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with IdM systems: Microsoft FIM 2010, IBM Tivoli IdM.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indeed ESSO TMS/SAM Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration eToken and the user account data lifecycles.</td>
</tr>
</tbody>
</table>

Contact and additional information

Our contacts:
- [inbox@indeed-id.com](mailto:inbox@indeed-id.com)

Our resources:
- site [indeed-id.com](http://indeed-id.com)
- video gallery [youtube.com/user/IndeedID](https://www.youtube.com/user/IndeedID)