INDECT Security Architecture

Manuel Urueña[1], Petr Machník[2], Marcin Niemiec[3], Nikolai Stoianov[4]

[1] Universidad Carlos III de Madrid, Department of Telematics Engineering,
Avda. Universidad 30, 28911 Leganés (Madrid) Spain, muruenya@it.uc3m.es;
[2] VSB-Technical University of Ostrava, Department of Telecommunications,
Listopadu 15, 708 33, Ostrava, Czech Republic, petr.machnik@vsb.cz;
[3] AGH University of Science and Technology, Department of Telecommunications,
Mickiewicza 30 Ave., 30-059 Krakow, Poland, niemiec@kt.agh.edu.pl;
[4] Technical University of Sofia, INDECT Project Team,
8, Kliment Ohridski St., 1000 Sofia, Bulgaria, nkl_stnv@tu-sofia.bg;

Abstract. In order to carry its duties to serve and protect, the Police must deploy new tools and applications to maintain the pace of technology evolution. The INDECT project is developing such novel investigation tools for European Police forces. However Police ICT systems have stringent security requirements that may delay the deployment of these new applications to first implement the required security measures. This paper presents an integrated security architecture that is able to provide common security services to both, novel and legacy ICT applications, while fulfilling the high security requirements of Police forces. By reusing the security services provided by this architecture, new systems do not have to implement custom security mechanisms themselves, and may be easily integrated into the existing Police ICT infrastructure. The proposed INDECT security architecture features state-of-the-art technologies, like encrypted communications at network and application levels, or multi-factor authentication based on certificates stored in Smart Cards.

Keywords: INDECT Project; Police ICT systems; Security.

1 Introduction

The continuous evolution of Information and Communication Technologies (ICT) has brought enormous changes to the world, where the Internet is a prime example of this progress. However organized crime has also embraced these new technologies and is increasingly employing them to perform criminal activities, in order to be one step ahead of the Law Enforcement Agencies (LEAs) that pursue them. Therefore Police forces must not lose the pace of technology evolution, and have to employ new tools to fight those new high-tech crimes, as well as to leverage ICT technologies to improve their investigations.

INDECT [1] (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*) is a research project funded by the EU 7th Framework Program that is developing cost-effective tools for helping

Multimedia Communications, Services & Security (MCSS'13), p. 1, 2013.

European Police services to enforce the law and guarantee the protection of their citizens. Thus the so-called INDECT system is composed by a set of novel applications and ICT services designed to help Police forces in their current investigations, as well as to fight new forms of cyber-crime.

Therefore Police forces are very interested in deploying these new tools as soon as possible in order to do not lag behind in the continuous arms race with organized crime. However, since the information handled Police forces during their investigations is extremely sensible (e.g. names of informants, protected witnesses, etc.), any new system to be deployed inside Police's ICT infrastructure must fist fulfill a stringent set of security requirements [2]. Therefore it is quite common that new tools must implement additional security mechanisms, which are usually custom made. This process may greatly delay the deployment of these new tools, and there is a important risk that those custom-made security mechanisms, added in a later stage of the development process, do not provide the adequate protection. Moreover, Police administrators have to manage a set of heterogeneous ICT systems with fairly different security mechanisms that cannot be easily integrated with other legacy applications or even into their normal operations (e.g. user management), which have to be modified to include each new application, further increasing the deployment delay.

In order to solve these problems, and given that there are no works in the public literature dealing with these problems with Police ICT systems, this paper presents an integrated security architecture in order to provide common security services (i.e. authentication, authorization, confidentiality, integrity, non-repudiation, auditing, etc.) for Police ICT systems, and thus being implemented with state-of-the-art security technologies. Although this architecture has been designed for the systems being developed inside the INDECT Project, it can be also employed for other Police ICT applications, including legacy ones.

2 INDECT Security Architecture

The proposed INDECT security architecture provides a set of common security services, which were previously defined in [2]. The set of common services provided by the INDECT Security Architecture include Authentication, Authorization (Access Control), Non-Repudiation, Privacy/Auditing, Communication Security, Data Confidentiality and Integrity. Other security services such as Efficiency, Reliability and Availability or common ICT security best practices are out of the scope of this paper because they greatly depend on the ICT environment they will be deployed in.

Although each INDECT application has its own security needs and characteristics, the proposed architecture includes a number of security infrastructures [3] that provide common security services using standardized protocols and mechanisms. Those security services are provided by means of a combination of novel and standard security protocols and mechanisms. Figure 1 shows a simplified view of the integrated INDECT Security Architecture for Police ICT systems.

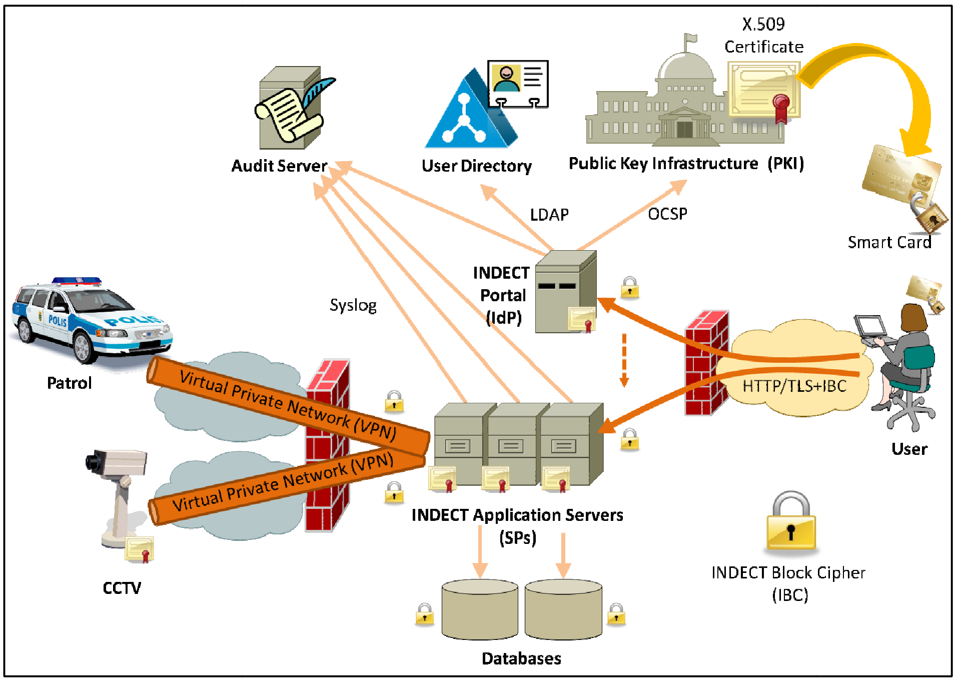

Fig. 1. INDECT Security Architecture

The main components of proposed INDECT Security Architecture are:

- **Public Key Infrastructure (PKI)** – to issue, mange, store and revoke X.509 certificates used in system. Certificates are issued to all INDECT users and ICT systems to authenticate them as well as to secure their communications.
- **LDAP User Directory** – to store all users' contact data and credentials for legacy systems that do not support certificate-based authentication. The user directory also stores general authorization information, such as the users' clearance level or the specific applications they can access to.
- **Audit Server** – all relevant user actions (e.g. accessing an application or requesting classified information) are logged both locally and in a secure centralized system. These logs are constantly being reviewed by security personnel and Police auditors in order to detect suspicious behaviours.
- **INDECT Portal** – is the homepage of Police users. It allows them to access the different services and applications available to them, according to particular scenarios (e.g. in a crisis). The INDECT portal will also act as the Identity Provider (IdP) of INDECT Federated-enabled systems. User authentication is based on X.509 certificates and/or user credentials stored at the LDAP User Directory.
- **INDECT Application Servers** – execute the different services, applications and tools being developed by the INDECT project. They may act as Federated Service Providers (SP), authenticating the users through the INDECT Portal (IdP) although they may also handle application-specific user's authorization attributes (e.g.

which CCTV cameras an given user may access to). Most INDECT applications provide a web-based interface, and most services are also web-based, implementing SOAP or REST interfaces, and using SSL/TLS for secure communications, featuring mutual client-server authentication.

- **INDECT Databases** – although stored deep inside the Police Data Center, they should communicate in a secure way with IDECT Application Servers and being encrypted, for instance using the novel INDECT cryptographic algorithms presented later. This also applies to all communications between INDECT subsystems, even if they are located in a Data Center with Police-grade physical security.
- **Virtual Private Networks (VPNs)** – protect the communications with external Police users and devices. Only encrypted traffic is allowed to go through the Police Data Center firewalls, which block all external traffic by default and should feature additional security mechanisms such as Intrusion Detection Systems (IDS).
- **Smart Cards (SC)** – storing users' certificates are issued by the INDECT PKI and used for access control by the central INDECT web portal, encrypt and sign e-mails and documents.

In order to guarantee the robustness of the security architecture and to support a wide support of applications, standard security protocols like TLS/SSL or IPSec have been preferred to proprietary or custom ones. Nonetheless the INDECT security architecture also includes novel mechanism such as the new INDECT Block Cipher (IBC) that may be employed to encrypt TLS/SSL sessions and VPN tunnels.

For a complete description of the proposed INDECT Security Architecture, the reader is referred to [4].

2.1 LDAP User Directory

Although it is recommended that all INDECT applications are based on the proposed Federated Identity Management, where the INDECT Portal acts as the Identity Provider (IdP) and thus authenticates all users, it is still possible that some applications, including legacy Police systems, do not implement Federated ID management or even certificate-based authentication. Therefore the INDECT Security Architecture also includes a LDAP Directory Service that stores users' information, including user credentials (i.e. login/password) for such legacy applications. A LDAP-based directory service has been selected because nowadays it is commonly employed by enterprises, including Law Enforcement Agencies, for user management (e.g. Windows Active Directory is based on LDAP). The proposed INDECT LDAP schema has been designed to be as standard as possible in order to be easily integrated in existing LDAP systems.

LDAP User Directory contains the information about all INDECT applications and users. This way it is possible to specify, in a centralized way, which applications can be accessed by each user, as well as to specify common authorization attributes of users. Legacy applications can then query the INDECT User Directory by means of LDAP commands in order to: (i) verify whether a user has access to that application or not, (ii) validate the authentication credentials provided by the user, and (iii) check the user's authorization attributes to enable only the allowed actions.

2.2 Audit Server

Given the sensitive information that Law Enforcement Agencies (LEAs) handle, and in order to protect the privacy of citizens, the operations of LEA agents are continuously monitored by a specialized department of auditors. However, the complexity of INDECT system would require LEA auditors and security personnel to check the logs of a huge number of systems and applications. Therefore the proposed INDECT security architecture also includes a centralized Audit Server that aggregates the logs of all INDECT subsystems. This way, LEA auditors and ICT security personnel only have to monitor a single log stream, with the additional benefit of easing the correlation of events from different systems, which could be easily missed with separated logs.

This centralized log server also provides benefits from a security point of view, because logs are stored in two places, locally at the Application Server and remotely at the Audit Server, which can only be accessed by LEA auditors and that does not support deleting log records. This way, even if a server is compromised and the attacker is able to erase its actions from the local log, by then they would be already stored at the Audit server and thus subject to auditors scrutiny. Therefore all relevant INDECT user actions and system events must be logged locally by the Application Server, as well as be sent to the centralized Audit Server. This also applies to remote applications, that may use VPN tunnels to send its log events to the Audit Server, either directly or through an INDECT Application Server acting as proxy.

For especially sensible operations (i.e. authorizing the wiretap of a suspect) and/or due to regulatory requirements, just logging those operations may be not enough. The details of such sensible operations must be cryptographically signed by the officer requesting/approving it for proper authorization and to ensure non-repudiation.

3 INDECT cryptographic algorithms

This section presents new cryptographic solutions that have been developed by the INDECT project. Currently, two novel symmetric ciphers (block and stream) as well as a hash function are ready to be used by end-users. Additionally, new high-level security methods for quantum cryptography have been proposed. These solutions are the significant part of INDECT security architecture.

3.1 INDECT Block Cipher (IBC)

Encryption of confidential data is the most important task of cryptography. It relies on transforming plain data into another encrypted form, unreadable to anyone except of those possessing the cryptographic key, by using an appropriate algorithm, called cipher.

Nowadays, there are many different ciphers. A well-known example is Advanced Encryption Standard (AES) that encrypts data using simple functions: substitutions with a single S-box, permutations, and adding the key. The INDECT project has further developed these ideas: employing more substitution boxes (S-boxes), using a cipher with dynamic structure, etc.

In general, the new cipher, called INDECT Block Cipher (IBC), consists of nonlinear transformations, which are dependent on the key [5]. This feature ensures a higher level of security. Additionally, the large number of secure S-boxes makes each encryption highly unique. The construction of this cipher is based on substitution and permutation functions that are used in each round of the IBC cipher. This structure ensures a good performance and a fast data encryption.

The IBC algorithm is a block cipher. Each 256-bit block of data is divided into 64 sub-blocks. Each sub-block is transformed by the appropriate substitution box and output values are concatenated into one 256-bit block. At the end of the round, the permutation function based on S-box, further modifies the 256-bit block of data. These steps are repeated for a number of iterations (e.g. a minimum of 8 times).

The novel idea of the IBC cipher is unique approach to key. The key is still a pseudo-random sequence, however it is used to create new S-boxes. These substitution boxes are based on the AES S-box, and ensure the same level of security. In this way, we can create about $5.35 \cdot 10^{18}$ new S-boxes from a single AES S-box. All new S-boxes represent a unique non-linear transformation: substitution or permutation. Because of S-box size, the cryptographic keys of IBC cipher must be a multiple of 64 bits. Four key lengths have been chosen for practical use:

- **128 bits** where two S-boxes are used: one for substitution and another for permutation. For 128-bit keys, eight rounds of cipher are proposed.
- **192 bits** where three S-boxes are used: two for substitution and one for permutation. For 192-bit keys, ten iterations of the cipher are proposed.
- **320 bits** where five S-boxes are used: four for substitution and one for permutation. For 320-bit keys, twelve rounds of the cipher are proposed.
- **576 bit**s where nine S-boxes are used: eight for substitution and one for permutation. For 576-bit keys, fourteen rounds of the cipher are proposed.

3.2 INDECT Stream Cipher (ISC)

Stream ciphers are able to encrypt a single bit (or byte) of data using a generated key. They are a class of symmetric ciphers that are based on the one-time pad principle. The main difference is that in one-time pad ciphers the key length must be equal to the message length, while stream ciphers employ a key with a much smaller length.

The INDECT Stream Cipher (ISC) provides two encryption modes: a keystream generation based on Linear Feedback Shift Registers (LFSRs), and a symmetric stream cipher based on the IBC cipher.

The keystream generator based on LFSRs uses 16 binary registers and one additional operating in the integer domain. All registers are initialized at the beginning of the encryption process with the provided key. Since the size of registers varies, the provided key is truncated each time before initialization in order to fit in a given register. The key size required for this encryption mode must be 256 bits long.

The stream cipher based on IBC is the solution where a block of data is encrypted by the IBC algorithm using two operation modes: Output Feedback (OFB) and Cipher Feedback (CFB), which may operate over bit or byte streams.

3.3 INDECT Hash Function (IHF)

Hash functions are a group of transformations where variable length data are transformed into a small, fixed-length digest. This transition must be one-way only and part of the original information is lost. Although these functions have a small probability of collision (i.e. when two different input data produce the same output) is almost impossible in practice.

A new hash function, called INDECT Hash Function (IHF), has been created by INDECT project. The hash function has a structure of substitution-permutation network, with different key lengths and different number of rounds. Therefore, this hash function provides different security levels. The design of IHF is based on the IBC algorithm using the CBC-MAC chaining mode. Thus, the key sizes and number of rounds proposed for the INDECT Hash Function are the same as in IBC.

3.4 Quantum cryptography methods

Quantum Cryptography (QC) is a new way of solving the key distribution problem for symmetric ciphers. It provides a secure key distribution service by means of the laws of quantum mechanics:

- any measurement modifies the state of the transmitted *qubit* (quantum bit) and this modification can be discovered by end-users,
- it is not possible to clone an unknown qubit (it is not possible to measure the quantum state and simultaneously send a cloned qubit to the real receiver).

Some new high-level quantum cryptography methods have been proposed [6] by the INDECT project, including the verification of the described solutions. This study is based on both theoretical analyses, as well as in a custom-developed simulator (the QKD Protocol Simulator) [7].

The new QC methods are based on the idea of measuring the security level during the QBER estimation and privacy amplification processes. Two new functions were proposed: a measure of security and entropy of security. They define the average security of the key when we uncover and compare a part of the exchanged key. Using these functions we can specify the security levels in a QC system. We propose two security levels: basic and advanced security. Thanks to these security levels we can personalize the security for specific end-users and services. Also, we have verified the methods by means of simulations, and have distributed a questionnaire of interest among potential end-users of QC systems.

4 INDECT Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is a common way to solve the problems related to the distribution of public keys, because it offers the scalability that is required for big communication and information infrastructures. A PKI is usually used to create policies, mechanisms and mechanisms for asymmetric key management, where public keys are distributed in the form of the so called digital certificates. However in INDECT the information that is included in certificates is more than just a public key since they are also employed for authentication and authorization purposes. Certificates are digitally signed to ensure the integrity and validity of the contained information [8].

4.1 Digital Certificates

A digital certificate is a representation of the link between the identity of a person or device and its corresponding digital information. This digital cryptographic information is comprised by the public keys of the subject. The digital certificate also contains other information related to people or devices, and this information is independently signed by the so-called Certification Authority (CA).

The basic elements of the INDECT PKI infrastructure are:

- **Root CA server** – is based on a self-signed (root) certificate, and it is always offline because it only issues the certificates of its Sub-CAs..
- **Users CA** (Subordinate certificate authority for users) – manages all certificates related to users. These certificates are stored on smart-cards to enable two-factor authentication.
- **Devices CA** (Subordinate certificate authority for devices) – manages all system certificates issued for devices. In the INDECT architecture devices could be: Servers, CCTVs, Users' PCs, Tablets, Smartphones, communication devices, etc.
- **Users RA** (Registration authority for users) - generates certificates from PKCS#10 requests, generates PKCS#12 for the end user, performs key recovery of the users‘ key (if requested using PKCS#12), edits users, revokes certificates, renews the certificates of existing users, generates a key storage for existing users, etc. The Users RA is operated by the EJBCA software package [9].
- **Devices RA** (Registration authority for devices) - generates certificates for devices, edits devices profiles, revokes certificates, renews certificates for existing devices. The Devices RA is also operated using the EJBCA software.

- **PKI Backup/Log Server** – for disaster-recovery procedures and for auditing the processes of certificate management. PKI logs are also copied into the global INDECT Audit Server.

The architecture of the deployed INDECT PKI infrastructure is shown in Figure 2.

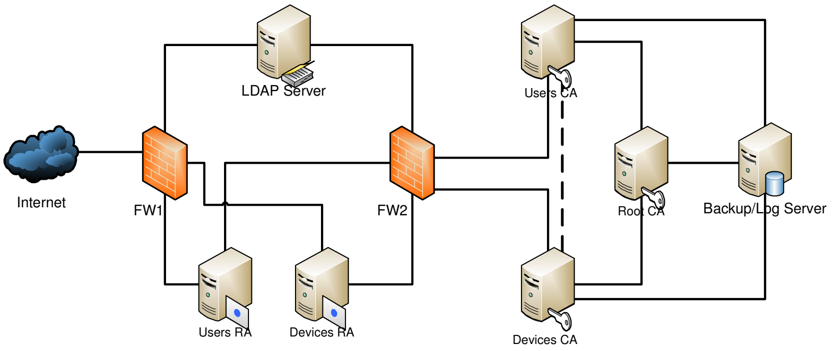

Fig. 2. INDECT Public Key Infrastructure (PKI)

The process for requesting and issuing certificates through a RA are as follows:

1. A certificate request is sent to the RA by a user.
2. The certificate request is checked and verified by the RA and stored locally.
3. The CA is waiting for certificate requests and periodically checks the RA database. It processes the request by issuing a certificate and stores it back to the RA's DB.
4. The RA periodically looks for new certificates issued by the CA.
5. The RA sends the new certificate to the user after processing it.

4.2 Certificate Revocation List (CRL)

Often some certificates must be revoked before certificates' validity periods expire, for instance if its private key is somehow compromised. In this case the CA must create a list of revoked certificates, called Certificate Revocation List (CRL). This list includes the serial number of the revoked certificate and the reason for its revocation. Up to date information about revoked certificates is critical for a healthy PKI system. Therefore, the proposed update time for the CRLs of the INDECT PKI is 5 minutes. Four settings should be also configured on EJBCA [9] (the CA software employed for managing certificates) to define how CRL generation is done:

- CRL Expire Period: This is the validity period of the generated CRL. It is set to 24 hours.
- CRL Issue Interval: This is the interval when the new CRL will be issued. For INDECT PKI it is set to 0, meaning that new CRL will be issued after old CRL is expired (24 h).

- CRL Overlap Time: This setting defines the time when the new CRL should be issued before the old CRL is expired. For INDECT PKI, the CRL Overlap Time is set to 10 minutes.
- Delta CRL Period: This setting defines the amount of time a Delta CRL (i.e. differences with a previous CRL) is valid after being issued.

4.3 Certificate extensions for INDECT users

Certificate extensions are optional by definition. This functionality was introduced in X.509 version 3. Based on these properties (extensions) it is possible to create a template and use it for issuing certificates for different purposes [8].

In INDECT peach police-officer has a unique identifier that is used for identification and stored in their certificates. The credentials of all users will be stored in LDAP repositories so for uniformity the UID (User ID) attribute is used for user identification in INDECT systems and thus this UID is also stored in certificates.

Additional information for rights management, such as the access level of users, is also stored in INDECT certificates. We assume the common security access levels: Unclassified, Restricted, Confidential, Secret and Top Secret. Therefore the certificate has an additional extension that stores the maximum access level of the user as follows:

- Unclassified access level: 0.
- Restricted access level: 1.
- Confidential access level: 2.
- Secret access level: 3.
- Top Secret access level: 4.

5 INDECT communications security

Given the distributed nature of the INDECT system, one of the main components of the secure communication infrastructure is a Virtual Private Network (VPN) framework that will enable the secure communication among multiple remote nodes and servers interconnected over public networks [4]. Nowadays VPNs are mostly based on two different technologies – SSL (Secure Socket Layer) and IPsec (Internet Protocol Security).

5.1 SSL VPNs

The best open-source SSL VPN solution is the OpenVPN software package [10]. OpenVPN can be installed in computers with most of current operating systems. OpenVPN is a very flexible and scalable VPN software. The advantages of OpenVPN SSL VPNs are as follows [11]:

- OpenVPN can be installed on various platforms – computers with Linux, Windows, or Mac OS X operating systems; smartphones with Windows Mobile, or Android (using CyanogenMod firmware) operating systems.
- OpenVPN offers two basic modes that run either as a layer 2 or layer 3 VPN. For example, OpenVPN layer 2 tunnels are able to transport Ethernet frames. Because of this ability, OpenVPN behaves more as an IPsec VPN, than a typical SSL one, which is mainly used for a secure web communication.
- Once OpenVPN has established a tunnel, the central firewall in the Police headquarters can protect the client device, even though it is not a local one.
- OpenVPN can use either TCP or UDP transport protocols and can work as a server or client. To improve the security level, a server can accept only connections initiated by clients within the specific virtual private network.
- Since OpenVPN 2.0, a special server mode allows multiple incoming connections on the same TCP or UDP port, while still using different configuration for every single connection. Thus, only one port in the firewall has to be opened.
- OpenVPN has no problems with Network Address Translation (NAT) and hence can be employed in networks with private IP addresses.
- OpenVPN offers many possibilities to start individual scripts during connection setup. These scripts can be utilized for a great variety of purposes like authentication or failover.
- Both tunnel endpoints can have dynamic IP addresses.

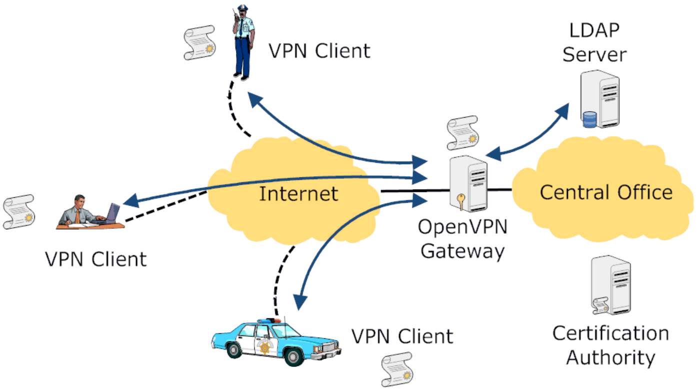

Fig. 3. Example of an OpenVPN network

Within the INDECT system, users will employ mainly OpenVPN to securely communicate between their remote terminals (desktop, laptop, tablet, smartphone, etc.) and servers located in the police headquarters (see Fig. 3). The INDECT Devices CA will be employed to authenticate the individual terminals.

To improve the security, so-called two-factor authentication mechanism can be employed. In that case, the user certificate is stored in a smart card or USB cryptographic token. Such a solution provides a strong user authentication, because the user needs to have the authenticator (smart card or USB token) and, concurrently, needs to know the password which protects the stored certificate from misusage.

To use these advanced authentication mechanisms, two open-source software packages exist that enable working with them – OpenSC and OpenCT. OpenSC [12] provides a set of libraries and utilities to work with smart cards and USB tokens. Its main focus is on authenticators that support cryptographic operations, and facilitate their use in security applications such as authentication, mail encryption and digital signatures. OpenSC implements the PKCS#11 API, so applications supporting this API (such as Mozilla Firefox and Thunderbird) can use it. On the card side, OpenSC implements the PKCS#15 standard and aims to be compatible with every software or card that does so too. OpenCT [13] implements drivers for several smart card readers and USB tokens. OpenCT also has a primitive mechanism to export smart card readers to remote devices via TCP/IP.

5.2 IPsec VPNs

The StrongSwan software package [14] provides an open-source IPsec VPN solution. StrongSwan is intended primarily for Linux devices. It is fully compatible with other standard IPsec VPN implementations, and thus can be used in networks with mixed equipment (see Fig. 4).

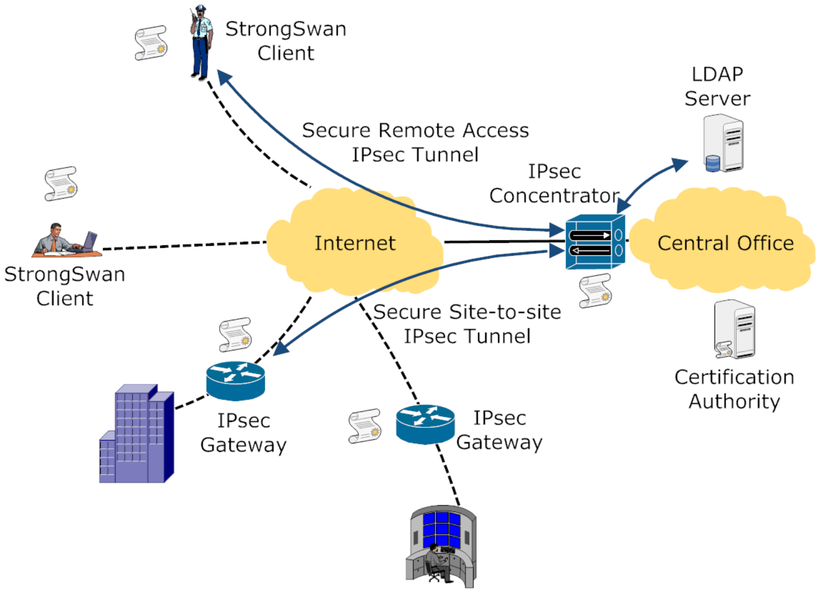

Fig. 4. IPsec VPN with StrongSwan clients

The main benefits of StrongSwan IPsec VPNs are as follows:

- StrongSwan supports various popular platforms – computers with Linux, Mac OS X, or FreeBSD operating systems; smartphones with the Android operating system.
- StrongSwan implements both IKEv1 and IKEv2 (Internet Key Exchange) protocols, and it fully supports IPv6.

- StrongSwan enables dynamic IP addresses and interface updates with IKEv2 Mobility and Multihoming Protocol, and IKEv2 Multiple Authentication Exchanges.
- It allows the automatic insertion and deletion of IPsec policy-based firewall rules.
- StrongSwan supports NAT-Traversal via UDP encapsulation and port floating.
- The XAUTH functionality is based on IKEv1 Main Mode authentication.
- The device authentication is based on X.509 certificates or pre-shared keys.
- StrongSwan enables secure IKEv2 EAP (Extensible Authentication Protocol) user authentication.
- RSA private keys and certificates can be stored on smart cards or USB tokens supporting the PKCS #11 interface.

5.3 Future work

The next step to achieve secure data communication via VPNs within the INDECT system is to evaluate the security and reliability of the proposed solutions in specific cases. Further, it is necessary to assess the compatibility of the proposed solutions in relation to the current solutions that are employed by the end users of the INDECT project (e.g., compatibility tests of IPsec tunnels based on StrongSwan and implementations based on commercial products). We also need to test cooperation of VPNs with other components of the INDECT Security Architecture in different situations and under different conditions.

6 Federated Identity Management

Federated ID management could greatly simplify all user-related security issues, such as authentication, authorization and auditing, by providing a common user management service to a set of cooperating organizations, usually called *circle of trust*.

In a Federated ID management system, all user-related information is centralized in the Identity Provided (IdP), so the Service Providers (SPs) does not have to manage any user information but just authenticate their users and obtain user information through the Identity Provider. This process is more secure, since users only need a single set of credentials. Moreover, it also enables the so called Single Sign-On (SSO), since users only have to authenticate once with the trusted IdP and then they can access any Federated Service Provider immediately, without any further authentication.

The proposed INDECT Security Architecture also includes Federated ID management functionalities, by means of the INDECT Portal that will act as the Identity Provider of INDECT users. Since all users have X.509 certificates (issued by the INDECT PKI and stored in Smart Cards), and the INDECT Portal is a secure (i.e. HTTPS) web server, users can securely log into the INDECT Portal using the TLS/SSL mutual authentication mechanisms, and therefore employing a secure two-factor authentication process.

Web-based applications can then act as Federated Service Identity Providers, and authenticate their users though the INDECT Portal (i.e. Identity Provider). For legacy applications that do not support Federated ID management, an LDAP user directory has been also deployed, which stores the credentials (i.e. login/password) and additional information of all Police users to ease its management.

Although Federated ID Management may also enable inter-organization cooperation, in this case the INDECT Security Architecture only applies to a single LEA. Given the different national legislations and specific LEA regulations, inter-LEA cooperation is not just a technical issue but a procedural one, and thus is out of the scope of this paper.

7 Conclusions

This paper has presented an integrated security architecture to allow European Law Enforcement Agencies (LEAs) to employ the novel tools and applications being developed by the INDECT project in a secure and reliable way. By providing common security services such as Federated ID management, it will be much easier to integrate new investigation tools into existing Police ICT systems, since it is only necessary to integrate the appropriate security service, instead of adapting each separate application. It is also worth noting that the proposed INDECT Security Architecture also considers legacy applications, which enables current Police ICT systems to be integrated into the proposed security architecture.

In particular, this paper has studied in detail the different security infrastructures, mechanisms and protocols that provide the main security services of such architecture. For instance, it has overviewed the novel cryptographic algorithms developed by INDECT project: the INDECT Block Cipher (IBC), the INDECT Stream Cipher (ISC), the INDECT Hash Function (IHF), as well as an analysis of the security level provided by quantum key distribution protocols.

One of the key characteristics of this architecture is the widespread usage of digital certificates to authenticate users and devices and to establish secure communications among them. Therefore the INDECT Public Key Infrastructure (PKI) is one of the main components of this solution. The INDECT PKI has a hierarchical structure with cross-certification, which enables all INDECT users and devices to be securely associated with an asymmetric key pair by means of digital certificates. Moreover, multi-factor authentication is supported by storing users' certificates in Smart Cards.

Secure communications are implemented by means of standard security protocols such as Virtual Private Networks (VPNs), supporting both SSL- and IPSec-based VPNs, and Transport Layer Security (TLS) that also leverages the digital certificates issued by the INDECT PKI for mutual authentication. The proposed INDECT Security Architecture also considers Federated ID Management. The INDECT Portal will act as the Identity Provider (IdP) of all INDECT users, while federated-enabled

INDECT subsystems will act as Service Providers (SPs), benefiting from a centralized and secure user authentication, as well as Single Sign-On (SSO) capabilities.

Acknowledgements

This work has been funded by the EU Project INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) — grant agreement number: 218086.

References

1. INDECT Project website: http://www.indect-project.eu [Accessed: February 1, 2013].
2. Manuel Urueña, Petr Machník, María J. Martínez, Marcin Niemiec, Nikolai Stoianov. "*INDECT Advanced Security Requirements*". IEEE Multimedia Communications, Services and Security (MCSS 2010), Krakow (Poland). May 6-7, 2010.
3. Nikolai Stoianov, Manuel Urueña, Marcin Niemiec, Petr Machník, Gema Maestro. "*Security Infrastructures: Towards the INDECT System Security*". IEEE Multimedia Communications, Services and Security (MCSS 2012), Krakow (Poland). May 31-June 1, 2012.
4. INDECT Consortium. "*D8.7: Definition of mechanisms and procedures for the security and privacy of the exchanged information*". January 2013.
5. Marcin Niemiec and Łukasz Machowski. "*A new symmetric block cipher based on key-dependent S-boxes*". International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT 2012), Saint Petersburg (Russia). October 3-5. 2012
6. Marcin Niemiec and Andrzej R. Pach. "*The measure of security in quantum cryptography*". IEEE Global Telecommunications Conference (GLOBECOM 2012), Anaheim (USA). December 3-7, 2012.
7. Marcin Niemiec, Łukasz Romański, Marcin Święty. "*Quantum cryptography protocol simulator*". IEEE Multimedia Communications, Services and Security (MCSS 2011), Krakow (Poland). June 2-3, 2011.
8. Carlisle Adams, Steve Lloyd. "*Understanding PKI: Concepts, Standards, and Deployment Considerations*", Second Edition, Addison Wesley, 2002, ISBN: 0-672-32391-5
9. EJBCA PKI website: http://ejbca.org [Accessed: February 1, 2013].
10. OpenVPN website: http://openvpn.net/index.php/open-source.html [Accessed: February 1, 2013].
11. M. Failner, N. Graf. "*Beginning OpenVPN 2.0.9*". Packt publishing, Birmingham, 2009.
12. OpenSC website: https://github.com/OpenSC/OpenSC/wiki [Accessed: February 1, 2013].
13. OpenCT website: https://github.com/OpenSC/openct/wiki [Accessed: February 1, 2013].
14. StrongSwan website: http://www.strongswan.org [Accessed: February 1, 2013].