Scentrics – what are we about?

- Scentrics has developed an innovative cyber-security solution, that is revolutionary for global communications and privacy, and which protects national security.
- The server-centric architecture lowers the cost of securing data at risk of compromise to hacking, while delivering full ease of use and a viral implementation expected to ensure rapid global acceptance.

Overview of system

Scentrics is a cloud-based key management system upon which a range of different security applications can be built. Currently implemented applications of the Scentrics key management system include:

- secure e-mail;
- mechanisms for secure messaging and cloud storage;
- mechanisms to support privacy for social network users (e.g. for users of Facebook).

Scentrics currently offers both key management and secure e-mail as a service via the Cloud. Current servers can be replicated on demand as load grows, thus ensuring scalability. A fundamental goal is to provide a single unified system for managing all the various types of key necessary to support both current and future use cases.

In addition to the cloud-based server, the Scentrics system also incorporates software running on a client platform (the *Scentrics client*). The role of the client software is to authenticate the user, retrieve the necessary keys from the Scentrics server, and store them for the lifetime of a session. The client software interacts with the client application to support the use of cryptographic functions as defined by the application (e.g. encryption/decryption and signing/verification of messages). For example it will interact with a native email application to encrypt (and decrypt) emails (and SMSes).

All keys are generated, distributed, revoked and managed at a central server, and not at the client. The client is responsible for use of the keys, e.g. for encryption of messages, so although key management is cloud-based, messaging security is end-to-end. That is, the server does not see and is not required to process individual messages; the solution thus scales because complex computations, such as encryption of individual messages, is distributed to the clients.

Cyber security – the need for solutions

Cyber security solutions are required to ensure protection of data against snooping and misuse, whilst also retaining simple and safe access and simultaneously providing support for national security. It is widely accepted that the current infrastructure of the internet does not meet these objectives, in large part because the internet was not designed with security in mind.

A pivotal problem that underpins these difficulties is that of cryptographic key management: how to put the right keys in the hands of the right people in a seamless and yet secure manner. The server-centric approach championed by Scentrics, protected by its patent and implemented in its product portfolio, provides a solution that delivers seamless cross-platform cyber security.

Scentrics is a UK company supported by an academic Technical Innovation Board (TIB) that has tackled this non-trivial task. The TIB includes leading scientists and engineers in the field who have defined the architecture and deployment strategy for the Scentrics 'core API' and its dependent applications, which can justifiably be described as 'disruptive'. The cloud-based Scentrics architecture matches that of telephony and enables the use of standard cryptographic methods whilst complying with legal and regulatory frameworks.

The purpose of this brief document is to provide a description of the motivating problem and to discuss the core ideas behind the Scentrics product portfolio.

Context

We start by examining the context within which the Scentrics key management service operates, and establishing the terminology we use throughout this document.

The protocol used to access the Scentrics key management service is designed to be used to enable *users* to make use of cryptographic services on a smart phone, tablet or PC in a mobile setting. That is, users wish to be able to make use of cryptographic services on any suitable device (we refer to the device currently employed by a user as the *client*). The main obstacle to achieving such mobility is ensuring that the user-specific cryptographic keys necessary for performing cryptographic functions are available at every platform.

In the Scentrics system, this is achieved with the aid of a trusted *server*. This server stores a *profile* for each user which it supports, where this profile contains all the security context information for the user (including cryptographic keys. certificates, and any other necessary user-specific information). The server is trusted to maintain the integrity and confidentiality of the profile. Part or all of the profile is transferred to a platform employed by the user, on request by the user (this transfer must take place in such a way that the confidentiality and integrity of the profile is preserved). The recipient platform can then use the profile to perform cryptographic functions for the user.

This profile transfer must take place in such a way that both passive and active interceptors are prevented from learning anything about the profile contents, and/or modifying the profile. This includes interceptors capable of performing so called *man-in-the-middle attacks*, in which an interceptor masquerades as the client to the server and the server to the client.

Of course, the server will need to have some means of authenticating the user before downloading the profile. For the purposes of this system, it is assumed that this will be performed using a secret password shared by the user and the server. This password may, at least in some cases, be a *weak secret*, i.e. be drawn from a relatively small set of possibilities, so that a well-informed attacker might be able to work through every possibility in this set in a feasible time.

In the remainder of this document we refer to a *session*, i.e. a specific period of time while a user is employing a particular client device. That is, the download of profile data will be required to support a session, and, even if a user has a number of sessions using the same client device, a profile download will be required on every occasion.

The client device is not necessarily completely trustworthy. Of course, if the software implementing the protocol has been manipulated then an attacker may be able to obtain a copy of the profile data downloaded to a client. This is a problem inherent to any application performing cryptographic processing on a client device. The likelihood of compromise is minimised in the Scentrics architecture by minimising the time during which keys are held on the client device; moreover, the impact of such a compromise could further be minimised by limiting the lifetime of the secret data that is downloaded to the client (including private and secret keys)[1]. The latter possibility is an inherent advantage on the cloud-based approach to key management. A further protection envisaged in the Scentrics patent portfolio is the use of a trusted execution environment at the client, where available, to perform critical security processing.

Rationale – the key management problem

A fundamental objective for cyber security is to protect the confidentiality and/or integrity of information, both when it is stored and when it is in transit. The information to be protected could include government or commercial secrets, health records for individuals, financial instruments, e.g. credit card numbers, and a host of types of personal information. The risks associated with a lack of appropriate protection are huge. For example:

- if an unencrypted commercially sensitive email is intercepted, then the potential consequences to the companies involved could be very significant, including potentially serious impacts on share price;
- users often store very sensitive personal information on social networking sites in unprotected form; these sites routinely mine user personal data for purposes which may be damaging to the end user; moreover such sites do not always delete data promptly, if ever;
- mobile devices are increasingly used for making payments and conducting m-commerce – if the integrity of individual transactions can be attacked then both individuals and payment organisations stand to lose very large sums of money.

Today, the means of communication in widespread use are often inherently insecure (e.g. the public Internet), and data is stored in the cloud on servers located around the world – often we are completely unaware of where our data is located. Routine data collection, generation, processing and management is performed on a wide range of platforms, many of which are inherently mobile (e.g. tablets and smart phones) and hence which can be easily lost or stolen. Against this background, the use of cryptographic techniques, such as encryption and digital signatures, to protect information is absolutely vital. Cryptography can be used to guarantee confidentiality, to enable detection of unauthorised changes, and to guarantee the origin of data. Indeed, cryptography is very widely used today in a huge range of applications, and is fundamental to the correct operation of computers and the Internet.

However, despite its success, there are major impediments to the full deployment of cryptography, especially to protect information managed by individuals. For example, whilst it is in theory possible for users to cryptographically protect sensitive emails so that they can only be read by their intended recipients, in practice this only happens in a small minority of cases.

[1] The lifetime of a downloaded private key could be limited by requiring the server to generate a new key pair for every session, and choosing a very short validity period (e.g. some small number of hours) for the key pair.

Similarly, whilst it is theoretically possible to use cryptography to protect stored data, the vast majority of individuals store data in the cloud, including on social media sites, completely unprotected.

The obvious question is 'Why?' That is, why don't users avail themselves of the many cryptographic products that exist to protect their data? The reason is clear – it is simply too difficult. The underlying problem is known as key management. Essentially, in order to use cryptography, users must generate secret keys, i.e. secret values (a little like passwords) which must be stored somewhere securely, since if the key is compromised then so is the data.

Ensuring appropriate management and storage of these keys is intrinsically difficult. Firstly, most user computers and phones do not have a secure place to store sensitive data, so that if the device is lost or stolen then the stored keys can be compromised. Secondly, to enable a protected message to be accessed, the appropriate keys somehow need to be transmitted to the recipients in a way that preserves their secrecy and integrity – this is highly problematic. Thirdly, the keys must be stored long term, since if a key is used to encrypt stored data and the key is lost, then the data cannot be decrypted, i.e. it is essentially gone forever. Fourthly, most users employ a variety of computers, including smart phones, tablets, notebooks and desktops, and if the key is stored on one device then it is typically not possible to access any protected data from another device.

The increasing use of mobile platforms means that any underlying security infrastructure must be lightweight, easily installed, and inherently flexible. Users expect to switch seamlessly between platforms, so, as noted above, solutions involving long-term storage of keys on user devices are almost bound to fail.

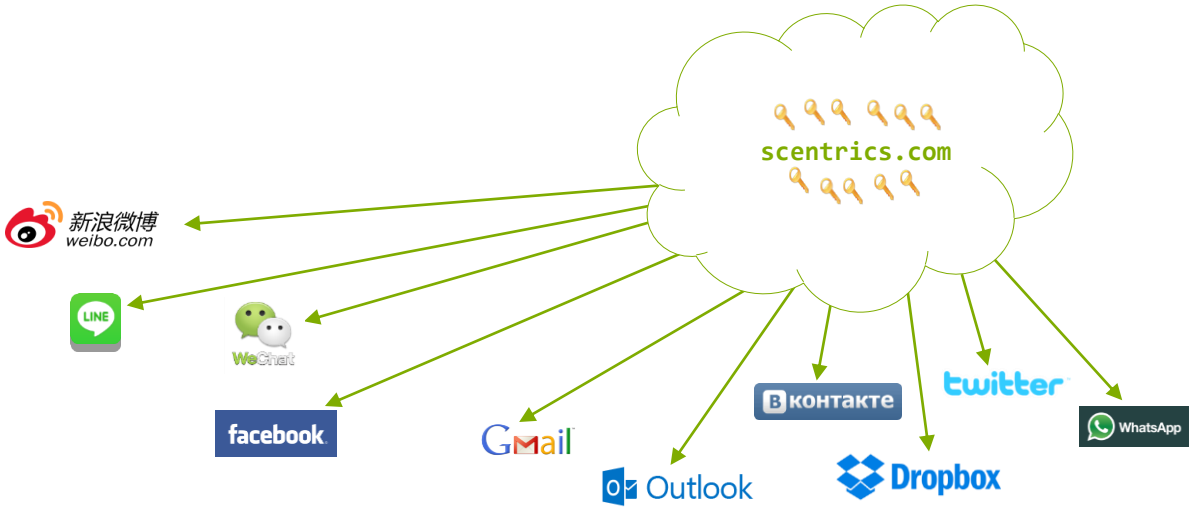
These are just some of the many practical barriers to the effective use of cryptography for the individual.

Innovation – the server-centric approach

The key innovation of Scentrics is to solve the key management problem in a way which:

- makes life extremely simple for the end user;
- transparently supports management and transport of keys between individuals;
- enables users to transparently use multiple platforms and still access their keys; and
- provides a secure and long term solution for key storage.

This is achieved by the deployment of the Scentrics cloud-based key management service. This service supports the full range of key management functionality, including key generation, key storage, key distribution, and key destruction, all under the control of the owner of the keys. The provision of this service by a known and trusted party (such as a telco) enables user confidence in the long term security and management of their cryptographic keys, and hence of their data. Most importantly, it enables users to *choose* who they trust, quite independently of what services they use for data storage and communication, i.e. it decouples the provision of data services and of trust that users' rights over data are respected.



Whenever a key is required, the user simply authenticates him/herself to the Scentrics server, and the keys are securely and automatically downloaded to the user's device. These keys are then used as necessary, and the local copies are deleted as soon as they are no longer required. This means that loss of a phone or tablet does not compromise keys, since they are never stored long term on devices. Keys cannot be lost since they are securely stored in the Scentrics key management server.

The key management functions provided by the Scentrics cloud service are complemented by software running on the user's platform. This software might, for example, take the form of a secure messaging application running on a user's phone, capable of seamless secure communication with a corresponding secure email application running on a PC or iPad. The client application communicates with the Scentrics cloud service using a standards-based secure protocol, enabling the process of user authentication and the download of keys to the client to be protected against both passive eavesdroppers and more active 'man in the middle' attackers. It is important to note that not only is the communications protocol standards-based, but all key management and cryptographic functions are also built on internationally agreed standards. This enables a high level of confidence to be derived in the security of the service.

It is also very important to note that the Scentrics key management service obviates the need for a Public Key Infrastructure (PKI). It is well-known that managing PKI functionality, including public key certificate generation, management and revocation, is a potentially costly and difficult task. Use of the Scentrics key management service thus offers significant cost and complexity reduction in comparison with the conventional approach of generating and storing keys long-term on user platforms, and supporting key distribution using a PKI.

By providing the key management service as a cloud-based service, administration of an entire domain of supported users becomes inherently straightforward. The Scentrics server provides a web-based management interface, allowing the set of users and their cryptographic keys to be managed both at an individual level and as a user population.

Support for lawful interception

The fact that the Scentrics service is cloud-based enables simple and secure management of keys in accordance with the prevailing legal framework, including lawful access to data. Depending on the laws applying within the jurisdiction in which the service operates, lawful access can be

given on a highly granular level to individual keys, e.g. enabling the decryption of individual protected data items or emails sent to or from a specified individual.

The instantiation of the Scentrics server supporting a particular service will be subject to the laws and regulations applying where it is located. That is, the operator of the server (such as a telco) will be able to both meet its legal obligations in a simple and seamless way, whilst providing guarantees to its users regarding the lawful handling of sensitive security-related material.

Impact – the basis for cross-platform cyber security

The range of applications for the Scentrics service is limited only by the imagination of developers. Any application, be it on a smart phone or a PC, which requires cryptography-based security can readily build on the robust and secure foundations provided by Scentrics. Scentrics has adopted a multifaceted approach to the development of applications based on its key management service.

1. Scentrics has developed a range of core applications building on its own service. Currently available applications include:

    - *secure email*, enabling secure interoperation between a range of device types (phones, tablets, PCs, etc.) running a range of operating systems (including iOS, Android and Windows);
    - *secure object encryption*, e.g. to enable secure storage of data objects in the cloud;
    - *social networking security*, enabling cryptography-enforced selective disclosure of user-sensitive pictures and messages.

2. Scentrics is also continuing to develop new applications building on its key management technology. A further application domain with rich potential is that of mobile payments, mobile money, and crypto-currency. In developing markets, payment applications running on mobile devices are growing rapidly, and look set to become the dominant means of electronic payment. Like all electronic payment schemes, security is critical for customer confidence, which itself is probably the primary factor determining the technology's growth. Security inevitably depends on the use of cryptography, which in turn relies on robust key management. Storing cryptographic keys long term on individual mobile devices is both a huge security risk and a barrier to cross-platform mobility – it is precisely these issues which the Scentrics technology solves.

3. Scentrics will provide specifications of the communications interface between the Scentrics cloud service and the client device to developers, enabling applications to be written that directly access the Scentrics key management service.

4. To greatly simplify the work of the developer, Scentrics also provide a client device software library, enabling simplified access to the Scentrics key management service for basic security functions such as message protection and object encryption. Not only will this avoid the application developer having to understand the complexities of cryptography and the details of the Scentrics communications protocol, but the library will offer the same interface across multiple device types, enabling simpler porting of applications from one device type to another.

Conclusions

The key innovation of Scentrics is to remove a major obstacle to the successful provision of data protection services to the end user, namely to solve the key management problem. These protection services are sorely needed in today's world, but without the Scentrics innovation providing them in a robust and simply way is an intractable problem.

The key management problem is solved in a way which:

- matches the telephony architecture with standards-based cryptography, allowing for national security and civil ethics to live in harmony with each other;
- allows for numerous business benefits for the mobile telecommunications service provider such as reduced churn and increased ARPU;
- makes life extremely simple for the end user;
- transparently supports management and transport of keys between individuals;
- enables users to transparently use multiple platforms and still access their keys; and
- provides a secure and long term solution for key storage.

This is achieved by the deployment of the Scentrics cloud-based key management service. This service supports the full range of key management functionality, including key generation, key storage, key distribution, and key destruction, all under the control of the owner of the keys. The provision of this service by a known and trusted party (i.e. a telco) enables user confidence in the long term security and management of their cryptographic keys, and hence of their data and services.

The Scentrics solution therefore provides a long-awaited architecture for the deployment and control of a standards based privacy scheme which can be applied to any number of instances and use cases. Primarily, the matching of the telco architecture is a main motivation behind its design and consequently the benefits derived by its deployment by a mobile telecommunications operator are only limited by its imagination.

For further information about Scentrics' cyber security solutions for Managed Network Operators, please email info@scentrics.uk.com