Secure Voice at OFFICIAL

Secure Voice at OFFICIAL
Version 1.0
November 2015

CESG
The Information Security Arm of GCHQ

About this document

This document provides an overview of secure voice technology for protecting OFFICIAL and OFFICIAL SENSITIVE communications.

Document history

Version	Date	Notes
1.0	November 2015	Initial version published on CESG Beta website.

Contact CESG

For additional hard copies of this document and general queries, please contact CESG using the following details:

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Email: enquiries@cesg.gsi.gov.uk
Tel: +44 (0)1242 709141

We welcome any feedback on this document.

Disclaimer

CESG provides advice and assistance on information security in support of UK government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not suitable for seeking appropriate tailored advice.

Contents

Section 1 Key principles

This section summarises some of the key principles for secure voice communications. For full details, see the Detailed Guidance section.

1.1 Risks to voice data

Voice data is subject to a number of key threats. These are summarised here:

- calls are placed to or received from an attacker and the user doesn't realise, resulting in compromise of spoken data
- attacker with privileged network access can access all call content and metadata for a user on that network
- attacker compromises a cellular base station, or uses a false base station, and gains access to all call content and metadata for all users on that base station
- attacker could cause calls to be routed via infrastructure they control (e.g. offering low-cost routing), enabling interception

1.2 What do I need to do to talk securely?

In the early 2000s, due to changing threats, the public telephone network (PSTN) was no longer considered suitable for RESTRICTED-level calls but only for UNCLASSIFIED. This caused an increase in demand for secure voice solutions.

Under the new government classification scheme, at OFFICIAL and OFFICIAL SENSITIVE, we therefore recommend the use of a CPA-approved solution to protect real-time communications. This includes voice, video and instant message communications. The CESG website contains a list of CPA-approved products.

1.3 What CESG approved products exist today?

As of November 2015, the following are available:

- CPA-approved secure voice applications are available for iOS and Android for use at OFFICIAL/OFFICIAL SENSITIVE.
- Further products are currently going through CPA assurance.
- Secure Chorus is a technology that allows secure voice products to interoperate. By adopting products which support Secure Chorus, users will be able to communicate with other users, companies or departments who have adopted Secure Chorus products.
- CESG has made it easy for communication product providers to integrate Secure Chorus into their products. There is an open-source code library, and the standards are documented by international standards bodies (IETF and 3GPP).
- CESG is committed to growing the Secure Chorus ecosystem to support more vendors and service providers. 4G Voice (VoLTE) will provide the perfect opportunity for service providers to offer end-to-end security to government and enterprise customers by adopting the Secure Chorus standard.

Section 2 Detailed guidance

2.1 History of secure voice

Under the previous protective marking scheme, the public telephone network (PSTN) was considered suitable for RESTRICTED telephone calls. However, as call routing has become more complex and unpredictable, local calls can be routed by a much longer path and over infrastructure controlled by a large number of third parties. Circuit-switched networks (where calls would always be routed the same way once established) have been replaced by packet-switched networks (where each data packet making up a fraction of a second of a call would each choose its own route). This has reduced confidence in the level of security provided by the PSTN and led to the network being regarded as suitable for UNCLASSIFIED calls only.

2.2 Do we need secure voice?

Those who have always used the PSTN for their calls may be sceptical of the need to 'go secure' when making voice calls because they have never historically been told to protect their voice data in transit. In contrast, they may be accustomed to protecting other data in transit using encryption. Arguably, voice data is just as important as the other the data we protect, and it is likely to prove harder to predict the sensitivity of discussions in advance. We previously did not widely protect voice communications because the technical challenge was too great, but this is no longer the case. The technology to provide true end-to-end security for voice traffic exists today and should be used to secure our communications.

2.3 The rise of VoIP

The evolution of the voice network away from circuit-switched routing coincided with the growth of Voice-over-IP (VoIP) services, where voice calls are encoded as data packets and sent over networks such as the Internet. This encapsulation lends itself well to encryption, especially end-to-end encryption if both ends of the connection support the same protocols.

A number of both open and proprietary VoIP standards were developed and made their way into commercial products. On the whole, open standards have not been as successful as their proprietary equivalents. This has resulted in isolated islands of VoIP connectivity: for example, users of Skype can call other Skype users, but not a FaceTime user.

In addition, as the details of the proprietary VoIP standards are not in the public domain, it is difficult to analyse them from a security perspective and therefore assess how well the technology meets the OFFICIAL threat model.

From a usability perspective, VoIP is very similar to making a normal voice call. This is usually done by running an application on general purpose hardware (e.g. an app on a smartphone), but it could also be done using specially built hardware. In both cases, user behaviour need not change to use VoIP instead of the public phone system.

From the network administrators' perspective, running a VoIP network requires the setting up of calling infrastructure such as SIP servers and gateways, or proprietary servers when proprietary products are used. When secure voice products are used, key management servers and/or certificate authorities will need to be set up and managed too.

The ability to support lawful interception and business practice monitoring is a key requirement of secure voice technology and it is often overlooked. Solutions which perform end-to-end encryption generally need to rely on key escrow to support lawful interception. Therefore telecommunications service providers are required to restrict their choice of technologies and/or run extra infrastructure in order to meet these obligations.

2.4 Developing scalable, secure voice

When we performed a survey of the technologies that were available in 2010, it became clear that none was wholly suited for use at scale at the OFFICIAL tier. So in consultation with leading cryptographers, and based on contemporary identity-based public key cryptography (IDPKC), a new open cryptography standard – MIKEY SAKKE – was developed and standardised in the IETF.

MIKEY SAKKE (Multimedia Internet KEYing – Sakai Kasahara Key Exchange) is different to classical Public Key Cryptography in that no certificates need to be distributed. Instead, a user's identity is their public key. Simply knowing a user's phone number is enough to establish a secure communications link with them. This is done using advanced elliptic-curve mathematics (developed in 2003), and we believe it is one of the first at-scale implementations of IDPKC in the world.

2.5 Decreasing cost, increasing availability

Traditionally, there has been a limited choice for secure products for government and they have been expensive and hard to procure. Because of the limited market and onerous certification schemes, products were frequently outdated. With MIKEY-SAKKE being an open standard, anyone is free to take the technology and integrate it into their product or application. This should ultimately increase the availability of products using the technology, thereby increasing competition and decreasing cost.

2.6 Secure Chorus: working towards interoperability

One key requirement for a secure voice ecosystem is that any person can call any other person in that ecosystem securely. There are no 'islands' of secure voice, isolated by the particular product or technology variant. To achieve this for government, Secure Chorus was developed. Secure Chorus contains MIKEY-SAKKE as the encryption algorithm at its core, but defines other protocols and codecs which Secure Chorus products must support.

Like other cryptographic algorithms such as AES, MIKEY-SAKKE defines a very small part of how a message between two parties is secured, and just as two products both using AES does not guarantee interoperability, two products using MIKEY-SAKKE does not either. Secure Chorus is more like TLS; it defines how two applications must talk to each other to ensure interoperability. Two products which support Secure Chorus will be able to communicate securely.

Secure Chorus is not the only way to create secure calls using MIKEY-SAKKE, but by adopting products which do support Secure Chorus, users are ensuring that they will be able to communicate with other users, companies or departments also adopting the standard. From a software developer's perspective, if they are trying to sell to UK Government for use at OFFICIAL, their product will need to go through a foundation grade assurance scheme to ensure that their product meets certain security requirements. Using Secure Chorus makes it very easy to meet many of those requirements.

There is also an open-source software library available for developers who wish to add Secure Chorus support to their products.

2.7 Interoperability with legacy voice products

VoIP has been around for many years now, and many organisations have already adopted the technology for use. Often, internal telephone systems are wholly VoIP-based, and these products cannot be upgraded to support Secure Chorus. To make use of these legacy devices in a secure way, standards and an assurance scheme for gateways have been produced. Gateways allow legacy products which support open standards such as SIP and RTP to communicate securely with Secure Chorus applications by passing their traffic through a gateway. The gateway encrypts and signs the traffic at the organisation's network boundary using Secure Chorus and then sends on the secured voice traffic to the Secure Chorus endpoint. In this way, new VoIP handsets need not be purchased for organisations who have already adopted VoIP for internal communications.

Note that if full end-to-end authentication and encryption is required, both parties will need to use a Secure Chorus product.

2.8 Assurance schemes for secure voice

To ensure that secure voice products are of an appropriate security standard for use by UK government, a CPA security characteristic and assessment process has been defined. This is for foundation grade; any certified products are appropriate for use at OFFICIAL and OFFICIAL SENSITIVE. Any product that uses MIKEY-SAKKE as its key exchange algorithm - and by extension Secure Chorus - can be entered for assessment. Products going for assessment can either be software applications for use on general purpose hardware (e.g. smartphone applications), or can be hardware devices (e.g. physical VoIP desk phone).

A list of certified Secure VoIP client and gateway products can be found at the CESG website.

2.9 Secure video, instant messaging and file transfer

Many Secure Chorus application vendors have added support for video calls, instant messaging and file transfer. These features can be used securely within the ecosystems provided by that vendor. However, these other protocols have not yet been standardised within the Secure Chorus framework, so there is no guarantee of interoperability between competing vendors' products. These features are on the road map for Secure Chorus, to ensure that all customers get the benefit of interoperability of these additional services.

2.10 What about other secure voice standards?

There are many other secure voice standards, such as ZRTP and SCIP. MIKEY-SAKKE and Secure Chorus were designed to meet a set of scale and usability requirements which, in our view, no other protocol was able to meet.

As a result we only developed standards, assurance schemes, and products for MIKEY-SAKKE. If organisations use other secure voice products, these can work with Secure Chorus products by using a gateway designed to interoperate with that alternative standard.

2.11 Current state of secure voice for government

As of November 2015, there is one CPA-approved secure voice product (Cryptify Call for iOS and Android); a further two are being evaluated. These vendors of these products are committing to supporting Secure Chorus in the next major release of their product. In addition, there are two Secure Chorus gateways which will be going into CPA assessment in the coming months.

CESG is committed to growing the ecosystem to support more vendors and service providers. 4G Voice (VoLTE) provides the perfect opportunity for service providers to offer end-to-end security at scale to government and enterprise customers by supporting the Secure Chorus standard.