MIKEY-SAKKE frequently asked questions

A brief guide to MIKEY-SAKKE, a protocol that allows organisations to provide secure communications with end-to-end encryption.

What is MIKEY-SAKKE?

MIKEY-SAKKE is a protocol designed for government and relevant enterprises to enable secure, cross-platform multimedia communications.

What are the advantages of MIKEY-SAKKE?

MIKEY-SAKKE is highly **scalable**, requiring no prior setup between users or distribution of user certificates. It is highly **flexible,** supporting both real-time communications (such as voice), conference calls, and deferred delivery (such as messaging and voicemail). It is designed to be **centrally managed**, giving a domain manager full control of the security of the system. But even so, it maintains **high availability**, as calling does not require interaction with centralised architecture.

What is MIKEY-SAKKE for?

MIKEY-SAKKE is designed to be deployed in an enterprise environment, particularly the government enterprise. Like other enterprise services, such as Blackberry's Enterprise Server and Microsoft's Active Directory (and other Kerbero-based authentication systems), it requires central management by the enterprise, in this case through a 'Key Management Server' (KMS). Once set up, it allows members of the government department or enterprise to communicate securely by providing their key material. To be clear, the security of the system is entirely controlled by the enterprise through the KMS.

Why does MIKEY-SAKKE exist?

NCSC recognised that there was a UK government requirement for secure communications. To achieve scale while maintaining competition, an open protocol was required which allowed companies to build interoperable solutions for government while competing on functionality.

How did NCSC define MIKEY-SAKKE?

NCSC defined MIKEY-SAKKE using an identity-based cryptographic protocol developed by two Japanese researchers (SAKAI and KASAHARA, 2003). Sakai-Kasahara (SK) is a well established IDPKC scheme. For authentication, NCSC used the elliptic curve digital signature algorithm (ECDSA), making minor adaptations to optimise use with the SAKAI-KASAHARA protocol. NCSC integrated these two protocols into the MIKEY framework to enable the protocol to support secure voice-over-IP (VoIP).

Do NCSC develop MIKEY-SAKKE security solutions?

No. MIKEY-SAKKE security solutions are not developed by NCSC. Instead, industry has developed solutions independently based on this open standard.

Who should use MIKEY-SAKKE?

MIKEY-SAKKE was primarily designed to support a government requirement for secure communications. It should be used where civil servants are discussing sensitive government business. This includes a range of applications including public safety. In many of these cases the employer also requires the ability to audit the secure communications through a managed and logged process. This

is particularly important for maintaining accountability in government. For example, should the actions of a police officer be investigated, the police force (and only the police force) needs to be able to decrypt the officer's communications.

Who else can use MIKEY-SAKKE?

Since developing the protocol, there has been interest from security-conscious enterprises with similar requirements. This includes financial, legal and health sectors.

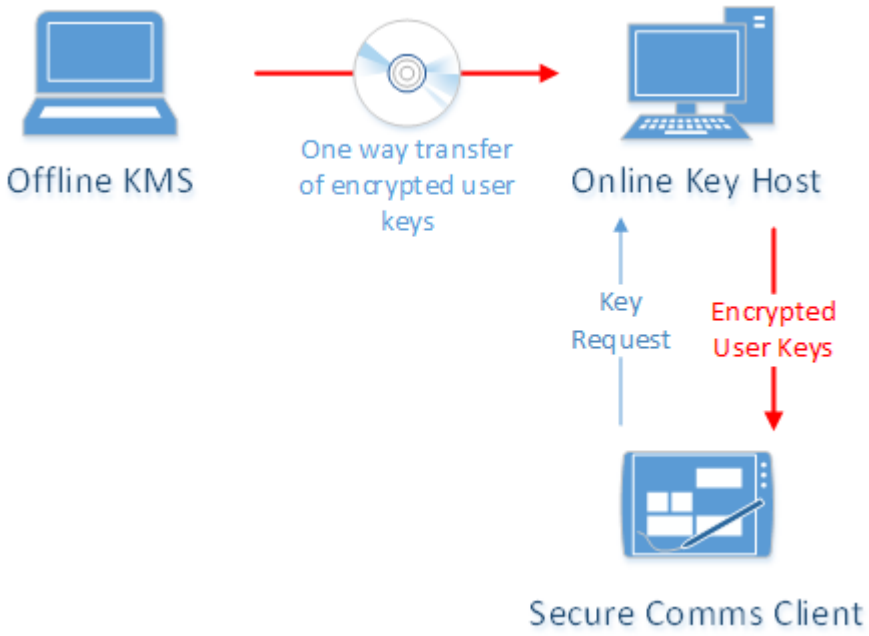
Is MIKEY-SAKKE secure?

MIKEY-SAKKE is secure provided it is deployed correctly. NCSC provides assurance that a correctly configured system prevents access to communications to even the most skilled adversaries. That is why NCSC are using it, and recommending it for wider use within the UK government. However, should the KMS be compromised, the security of all users managed by the KMS is compromised. This is true of all centralised architectures, including Microsoft's Active Directory, Blackberry's Enterprise Server and the Certificate Authorities which manage traditional Public Key Infrastructure. Hence, it is essential that the KMS is owned and managed by the system owner which owns the communications that it protects, and that the system is deployed in a way which prevents KMS compromise.

How should MIKEY-SAKKE be deployed in standard deployments?

To prevent KMS compromise, the KMS should be deployed so it cannot be reached by an attacker. The simplest approach is to deploy the KMS in 'offline

mode'. In this case, the KMS is held on a laptop which is never connected to any network and held in a secure location. User keys are transferred encrypted from the offline KMS to clients (e.g. via DVD upload to a distribution server). The KMS is protected from cyber attack as there is no way for an attacker to send any data to the KMS.



How should MIKEY-SAKKE be deployed in larger deployments?

For larger deployments, the KMS can be deployed within a Hardware Security Module (HSM) behind an assured diode, which only allows specific data to pass out from the KMS, and no data to be passed back. Again, the KMS is protected by preventing the attacker any access to the system. To further protect the KMS, the key material can be split across multiple servers, requiring an attacker to compromise multiple servers to be successful. Note that the KMS is the only component of the solution that the system owner would manage itself. As all client communications are encrypted, their communications can be routed over external VoIP services, such as those hosted by an ISP or mobile network operator.

Does MIKEY-SAKKE support audit or lawful intercept?

Yes, if allowed by the deploying department or organisation. This is a requirement for use in government and was explicitly built into the design of the protocol. To audit an encrypted communication, the organisation should export a user-specific and time-bounded key from the KMS. This key enables an audit function to decrypt that specific user's communications for that specific time period (e.g. month). The KMS is able to log this action to ensure that it is accountable.

Does the audit mechanism support mass surveillance?

No, as commercial KMSs will only provide time-bounded, single-user keys. To reiterate, the system owner is able to control their own KMS and hence control this audit function. Audit is not possible without knowing co-operation from the system owner. Similarly, should an organisation be issued with an appropriate warrant as part of a lawful interception request (e.g. as part of an insider trading investigation), the organization would be able to decide whether or not to provide the user-specific and time-bounded key to support that investigation.

Is the audit mechanism a backdoor?

No. In the same way, asking you for your login password is not a 'backdoor' to your laptop. The audit mechanism is a feature available to the system owner which may or may not be enabled. Should the organisation not require it, then the system owner can decide never to release the user key material. In this case, no one can decrypt the organisation's communications. In any case there is no 'backdoor'.

Are keys escrowed to GCHQ?

No.

Should my organisation use MIKEY-SAKKE if I don't trust the system owner that manages our KMS?

No. As the KMS manages your keys, it should be managed by someone who you trust.

PUBLISHED

7 August 2016

REVIEWED

7 August 2016

VERSION

1.0

WRITTEN FOR

Large organisations

Public sector