The hypocrisy of encryption products served in the UK

Written by Adison Verlice
Publication date:
2-11-2025
Description:
In this document, we talk about the hypocrisy of encryption in the United kingdom.

Context

Before we can begin to talk about this, we need to understand what encryption is.
Encryption is how you secure information, from your medical information, to your banking information.
However, in this context, we are talking about end to end encryption.
End-to -end encryption is an encryption mechanism where only 2 parties have an encryption key, and only those 2parties have that key. No government organization, no company, just you and the person you are talking with.

What is a backdoor

A backdoor is a third key, a key that would give someone else not part of your conversation access to that conversation.
A backdoor can be implemented by anyone, from government organizations, to your corporation/work (if they want to see work information), to people with malicious intent.

Ok that’s great, but why are you telling us this?

On 2-7-2025, BBC reported the united kingdom's intent to backdoor encryption by wanting to obtain backdoor access to apple users who use advanced data protection
Author:
Zoe Kleinman
Published on:
2-7-2025
From the text:
“The UK government has demanded to be able to access encrypted data stored by Apple users worldwide in its cloud service.”

Now we're not gonna talk about the implications of this, but what we will talk about is the UK government's hypocrisy on encryption products.
In this specific document, we are going to look at the national cybersecurity center (NCSC) of the UK.
“ “

Specifically, we will be taking a look at their catalog of products and services that work with the government.
Note
Words like, encryption, will have parentheses to make sure you won't miss it.
I will link to the products and services mentioned in this document so you can look for yourself.

motorola solutions UK

Let's see.
I wonder what this company is authorized to do.
Hmmmmm…

> Packet Data (Encryption) Gateway/Mobile Data (Encryption) Gateway
> Short Data (Encryption) Gateway
>
> Enhanced Grade Console
>
> Enhanced Grade (KMF)(Key Management Facility)

You may be wondering, why did I put “KMF” (even though the key management facility was already parenthesised) inside the document?
This is an important factor in encryption

What is a key management facility?

according to motorola solutions,

“The Key Management Facility (KMF) is a Project 25-compliant mission critical enterprise solution that can facilitate secure key management and distribution. It enables effective planning, implementation, and execution of security doctrine — all adaptable to user requirements. The KMF is composed of: (1) Windows® 2016 Server; (2) KMF Server and Client Software; (3) Windows 10 Client; and (4) KMF (CRYPTR).
Again, we are putting cryptr in parentheses because it is for importing encryption keys.
As you saw from the NCSC link above, the NCSC uses this to facilitate the management of encryption keys.

There's even a page at the national cybersecurity center (NCSC) that literally talks about this too.
From their text:
"The Motorola Enhanced Grade KMF offers the capability to import, allocate and then transfer keys to either a Key Loader (e.g. KVL3000 plus) or send keys over-the-air in order to fill an Airwave TETRA terminal. It also provides over-the-air configuration and management (key associations (crypto)period advancement and Stun or Kill) of terminals.
The terminal consists of an application running on a server and a dedicated hardware (encryption)engine (Motorola CryptR). It is also possible to run client applications on further PCs and remote working is possible with the appropriate protective measures."

I think I've made my point with motorola. Now onto another company working with the UK on encryption

ECTOCRYP® Yellow by Airbus Defence & Space

Information form the link

"**Details**

Type of product or service

Communications security - IP PRIME

Grade

TOP SECRET

Version

2.2

Ectocryp® Yellow is the next stage in sovereign UK (cryptography). Portable and low cost, Ectocryp® Yellow is the interoperable basis for highly secure strategic and tactical networks. Building on the success of Ectocryp® Blue, Ectocryp® Yellow is designed to provide the very highest levels of security for Governments and Defence customers.

Version 2.2 supports features to reduce system configuration overheads. The PRIME Peer Topology Sharing (PTS) feature enables PRIME (crypto)discovery and the support for OSPF/RIP on the plaintext network enables local topology discovery.

Key features

Sovereign High Grade SECRET and TOP SECRET

PRIME Suite A certified to interoperate with other certificated PRIME conformant devices, modules include:

- Base (IKE-V2)
- Suite A
- Pre-Shared Key

Pre Placed Key SA

Community Separation (CCOI)

NAT Traversal

DHCP CT

Peer Topology Sharing (PTS)

Advanced Networking

DSCP Bypass

IKEv2 Liveness

(Encryption)of multicast communications using Pre-Placed Key (PPK).

Supports OSPF/RIP routing protocols on the plaintext network.

Support for remote management simplifies management.

(Crypto) Ignition Key (CIK) supports easing handling constraints.

(Device OFFICIAL ACCESS when CIK removed)

Fully in field reprogrammable (via Encrypted software update).

Fully programmable platform to support future enhancements.

Tamper detection & Tamper evident seals.“

Withsecure

Now if you look closely, you’ll know that Withsecure indirectly is not assured to provide encryption services.

“Assured to provide

Cyber Incident Response (CIR)

CHECK Penetration Testing“

However,

Withsecure does have encryption products listed on their webpage.

1 in particular is called USB armory

From the text.

“

Contact us

The USB armory is the world's smallest secure computer.

It can safeguard data and run trusted applications, preventing unauthorized access or execution. Minimal attack surface, vast performance and capabilities. Fits right in your pocket, your laptop, your servers.”

So what does this have to do with encryption?

Note that i have taken out the extra headings so it is easier for you to read

“(Encrypted)storage solutions

Hardware Security Module (HSM)

Enhanced smart cards

Electronic vaults

e.g., cryptocurrency wallets, e-voting

Key escrow services

Authentication, provisioning, licensing, tokens”

USB firewall”

So yes, withsecure is providing encryption solutions.

The government could use those without our knowledge if they wanted to.

Conclusion

The government's public stance on encryption is different from the stance that the government itself has on its own use of encryption.
As we just saw, they use a number of different encryption products, and they will encrypt their own data, while we have to be backdoored and have our encryption broken into
End of document