

UDAQ item referenced from automated results

[REDACTED]

Hello Mr. [REDACTED] , "

What is the decrypted value of this KI?

...

[REDACTED] wrote:
> "Dear [REDACTED] , "
> "Yes after encryption i can find like this
> "IMSI: [REDACTED] = " , "KI : [REDACTED].
> "still there is authentication problem" , ".. we experienced like this problem when IMSI " , "are not match with correct KI.
> " , "
> "

"Subject: Re: OUTPUT FILE FOR 8 PCS SAMPLES --URGENT!!!

"Hello Mr [REDACTED] , "
> " , "
> "Just 1 thing to confirm" , "since you say IMSI and KI does not match but
> " , "over here I have rechecked and rechecked everything. I need to confirm
> " , "with you what is the KI that you get after decryption in your backend
> " , "system (after loading output file). So for example" , "
> " , "
> "

"1. IMSI: [REDACTED]
> " ,

"2. KI (randomly generated by us) - Clear value NOT encrypted :
> " , "[REDACTED]
> " ,

"3. KI (encrypted by transport key using DES CBC) :
> " , "[REDACTED]
> " ,

"
> " , "So" , "when " , "you load output file and then the back end system " , "decrypts" , "
> " , "is the value the same as above??
> " , "
> " , "Best Regards" , "
> " , "[REDACTED]
> "

CCNE "We penetrate targets' defences."



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on (non-sec) or email

© Crown Copyright. All rights reserved.