UPSC MAINS · ANSWER PRACTICE

Defence & Security · GS - III

“डिजिटल ट्रस्ट
इन्फ्रास्ट्रक्चर में साइबर
सुरक्षा की विफलताओं के परिणाम
उस संगठन तक सीमित नहीं रहते ,
जहाँ से वे उत्पन्न होती हैं। ”
eMudhra के सर्टिफिकेट -सुरक्षा
मामले के संदर्भ में चर्चा
कीजिए। भारत के डिजिटल ट्रस्ट
इकोसिस्टम को मजबूत करने के
उपाय सुझाइए।

EXAM YEAR

Daily Practice 23/10/2026

PAPER

GS - III

SUBJECT

Defence & Security

MARKS

10

WORD LIMIT

~150 words

Answer Hint
कमजोर क्रिप्टोग्राफिक कुंजियाँ , सर्टिफिकेट अथॉरिटी से
जुड़े जोखिम , फर्जी वेबसाइटों की संभावना , ऑडिट की कमियाँ और
सप्लाई -चेन की कमजोरियाँ मजबूत कुंजी प्रबंधन , स्वतंत्र ऑडिट
, त्वरित निरस्तीकरण , CERT-In समन्वय और जवाबदेही की आवश्यकता
दर्शाती हैं।

Model Answer
डिजिटल ट्रस्ट इन्फ्रास्ट्रक्चर वेबसाइटों , सॉफ्टवेयर और
उपयोगकर्ताओं की पहचान सत्यापित करके सुरक्षित ऑनलाइन लेन -देन
सुनिश्चित करता है। eMudhra का मामला इस महत्वपूर्ण व्यवस्था की
कमजोरियों को उजागर करता है।

www.becomeias.com YouTube: becomIAS | Instagram: howtobecomeias

अक्टूबर 2026 में eMudhra के अंतरराष्ट्रीय
वेबसाइट -सुरक्षा व्यवसाय से जुड़ी आठ
इंटरमीडिएट सर्टिफिकेट अथॉरिटीज़ की
क्रिप्टोग्राफिक निजी कुंजियों में
कमजोरियाँ पाई गईं। कुंजी निर्माण में
त्रुटि के कारण इन कुंजियों के दुरुपयोग से
फर्जी सर्टिफिकेट जारी करने, वेबसाइट की
नकल करने और मैन -इन -द -मिडल हमलों का जोखिम
उत्पन्न हो सकता था। हालाँकि , किसी
वास्तविक दुर्भावनापूर्ण दुरुपयोग या
डेटा उल्लंघन की पुष्टि नहीं हुई।
अधिकारियों ने भारत की विनियमित डिजिटल
सिग्नेचर सर्टिफिकेट और eSign सेवाओं को
अप्रभावित बताया।

यह घटना कुंजी प्रबंधन , ऑडिट की
प्रभावशीलता , नियामकीय निगरानी और
विश्वसनीय मध्यस्थों पर निर्भरता से जुड़े
प्रश्न उठाती है।

भारत को स्वतंत्र सुरक्षा ऑडिट, सुरक्षित
कुंजी निर्माण , निरंतर जोखिम आकलन और
सर्टिफिकेट के त्वरित निरस्तीकरण को मजबूत
करना चाहिए। CERT-In, नियामकों और तकनीकी
कंपनियों के बीच बेहतर समन्वय तथा
पारदर्शिता आवश्यक है।

अंततः , डिजिटल शासन के लिए केवल डिजिटल
पहुँच नहीं, बल्कि सुरक्षा , जवाबदेही और
जनविश्वास भी अनिवार्य हैं।

www.becomeias.com YouTube: becomIAS | Instagram: howtobecomeias