

Germany-Bonn: IT services: consulting, software development, Internet and support

OJ S 174/2023 11/09/2023

Contract award notice

Services

Legal Basis:

Directive 2014/24/EU

Section I: Contracting authority

I.1. Name and addresses

Official name: Bundesamt für Sicherheit in der Informationstechnik

Postal address: Postfach 200363

Town: Bonn

NUTS code: DEA22 Bonn, Kreisfreie Stadt

Postal code: 53133

Country: Germany

E-mail: vergabestelle@bsi.bund.de

Internet address(es):

Main address: <https://www.bsi.bund.de>

I.4. Type of the contracting authority

Ministry or any other national or federal authority, including their regional or local subdivisions

I.5. Main activity

General public services

Section II: Object

II.1. Scope of the procurement

II.1.1. Title

Projekt 496 Teilprojekt 2: KI-Methoden in der Seitenkanalanalyse (KISKA)

Reference number: P496 TP2

II.1.2. Main CPV code

72000000 IT services: consulting, software development, Internet and support

II.1.3. Type of contract

Services

II.1.4. Short description

Im Rahmen des Projektes wird ein Überblick über existierende KI-Ansätze im Bereich der Seitenkanalanalyse gewonnen, mit Schwerpunkt auf asymmetrischen und ggfs. asymmetrischen Post-Quanten Verfahren. Dazu werden zunächst bisherige Veröffentlichungen und entsprechende Forschungsansätze auf diesem Gebiet zusammengefasst und anschließend Gemeinsamkeiten, Unterschiede und potentielle Schwierigkeiten im Vergleich zur symmetrischen Seitenkanalanalyse mit KI-Methoden, wo es bereits deutlich mehr Resultate und Veröffentlichungen gibt, ausgearbeitet. Es werden sowohl „klassische“ Machine Learning Verfahren (z.B. Random Forest, Support Vektor Machines, Decision Trees, Gradient Boosting, Naive Bayes, Template Attack) als auch neuronale Netze

(z.B. Multi Layer Perceptron, Convolutional Neural Network, Residual Neural Network) berücksichtigt.

In einem weiteren Schritt wird experimentell analysiert, welche KI-Ansätze aus dem Bereich der symmetrischen Kryptographie übernommen oder ggf. angepasst werden können und wo generell Unterschiede zwischen symmetrischen und asymmetrischen Methoden bestehen, die den Entwurf neuer Methoden nötig machen. Derartige neue Ansätze werden gemeinsam mit dem Auftraggeber entwickelt und erprobt, wobei der Fokus auf Power/EM-Seitenkanalattacken liegen wird. Insbesondere werden dazu geeignete Datensätze (Seitenkanaltraces und zugehörige Daten) erzeugt, die sich für das Testen und Benchmarking verschiedener Verfahren eignen. Für die Akquise der Testdaten werden relevante Verfahren verwendet, die in unterschiedlichem Maße durch dem Stand der Technik entsprechende Gegenmaßnahmen geschützt sind, so dass verschieden anspruchsvolle Angriffsszenarien entstehen. Im Rahmen der Experimente mit neuronalen Netzen werden ferner die Aspekte „Leakage-Attribution“, d.h. die Analyse, welche Informationen neuronale Netze ausnutzen, sowie die Studie adversarieller Beispiele berücksichtigt. Auch die Verwendung synthetischer Daten (z.B. adversarielle Beispiele, Data Augmentation, simulierte Traces, Traces mit künstlich eingefügtem Jitter etc.) zur Verbesserung von Seitenkanalattacken oder zur Extraktion von Informationen über Schwachstellen untersuchter Implementierungen ist zu untersuchen.

Bei der Auswertung der Ergebnisse werden unter anderem KI-Methoden mit den derzeitig verwendeten, „klassischen“ Methoden verglichen und es wird auf die Frage eingegangen, ob KI-Methoden klassischen Methoden in bestimmten Aspekten über- oder unterlegen sind und ob man beide Ansätze ggf. gewinnbringend kombinieren kann.

Die Ergebnisse des Projekts werden in eine Tool-Box von KI-Methoden münden, die unterstützend für die Seitenkanalanalyse von asymmetrischen (und ggf. asymmetrischen Post-Quanten) Verfahren genutzt werden kann.

II.1.6. Information about lots

This contract is divided into lots: no

II.1.7. Total value of the procurement

Value excluding VAT: 478 618,00 EUR

II.2. Description

II.2.2. Additional CPV code(s)

72000000 IT services: consulting, software development, Internet and support

II.2.3. Place of performance

NUTS code: DEA22 Bonn, Kreisfreie Stadt

Main site or place of performance: Beim Auftragnehmer

II.2.4. Description of the procurement

Siehe Abschnitt II.1.4).

II.2.5. Award criteria

Price

II.2.11. Information about options

Options: no

II.2.13. Information about European Union funds

The procurement is related to a project and/or programme financed by European Union funds:
no

II.2.14. Additional information

Section IV: Procedure

IV.1. Description

IV.1.1. Type of procedure

Open procedure

IV.1.3. Information about a framework agreement or a dynamic purchasing system

IV.1.8. Information about the Government Procurement Agreement (GPA)

The procurement is covered by the Government Procurement Agreement: no

IV.2. Administrative information

IV.2.1. Previous publication concerning this procedure

Notice number in the OJ S: [2023/S 101-315521](#)

IV.2.8. Information about termination of dynamic purchasing system

IV.2.9. Information about termination of call for competition in the form of a prior information notice

Section V: Award of contract

Contract No: P496 TP2

Title:

Projekt 496 Teilprojekt 2: KI-Methoden in der Seitenkanalanalyse (KISKA)

A contract/lot is awarded: yes

V.2. Award of contract

V.2.1. Date of conclusion of the contract

25/07/2023

V.2.2. Information about tenders

Number of tenders received: 3

Number of tenders received from SMEs: 3

Number of tenders received from tenderers from other EU Member States: 3

Number of tenders received from tenderers from non-EU Member States: 0

Number of tenders received by electronic means: 3

The contract has been awarded to a group of economic operators: no

V.2.3. Name and address of the contractor

Official name: cryptosolutions UG

Postal address: An der Ziegelei 17

Town: Essen

NUTS code: DEA13 Essen, Kreisfreie Stadt

Postal code: 45133

Country: Germany

The contractor is an SME: yes

V.2.4. Information on value of the contract/lot

Initial estimated total value of the contract/lot: 478 618,00 EUR

Total value of the contract/lot: 478 618,00 EUR

V.2.5. Information about subcontracting

Section VI: Complementary information

VI.3. Additional information

VI.4. Procedures for review

VI.4.1. Review body

Official name: Vergabekammer des Bundes beim Bundeskartellamt

Postal address: Villemombler Str. 76

Town: Bonn

Postal code: 53123

Country: Germany

E-mail: info@bundeskartellamt.bund.de

Telephone: +49 228-94990

Fax: +49 228-9499400

Internet address: <http://www.bundeskartellamt.de>

VI.4.3. Review procedure

Precise information on deadline(s) for review procedures:

Unternehmen haben Anspruch darauf, dass das BSI die Bestimmungen über das Vergabeverfahren einhält, vgl. § 97 Abs. 6 Gesetz gegen Wettbewerbsbeschränkungen (GWB). Rechte aus § 97 Abs. 6 GWB sowie sonstige Ansprüche gegen das BSI, die auf die Vornahme oder das Unterlassen einer Handlung in einem Vergabeverfahren gerichtet sind, können nur vor den

Vergabekammern und dem Beschwerdegericht geltend gemacht werden, § 156 Abs. 2 GWB. Die Vergabekammer leitet ein Nachprüfungsverfahren nur auf Antrag ein, § 160 Abs. 1 GWB. Es wird darüber belehrt, dass ein solcher Nachprüfungsantrag gemäß § 160 Abs. 3 Satz 1 GWB unzulässig ist, soweit

1. der Antragsteller den geltend gemachten Verstoß gegen Vergabevorschriften vor Einreichen des Nachprüfungsantrags erkannt und gegenüber dem BSI nicht innerhalb einer Frist von zehn Kalendertagen gerügt hat; der Ablauf der Frist nach § 134 Absatz 2 GWB bleibt unberührt,
2. Verstöße gegen Vergabevorschriften, die aufgrund der Bekanntmachung erkennbar sind, nicht spätestens bis zum Ablauf der in der Bekanntmachung benannten Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem BSI gerügt werden,
3. Verstöße gegen Vergabevorschriften, die erst in den Vergabeunterlagen erkennbar sind, nicht spätestens bis zum Ablauf der Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem BSI gerügt werden,
4. mehr als 15 Kalendertage nach Eingang der Mitteilung des BSI, einer Rüge nicht abhelfen zu wollen, vergangen sind.

Die o.g. vier Unzulässigkeitsgründe gelten gemäß § 160 Abs. 3 Satz 2 GWB nicht bei einem Antrag auf Feststellung der Unwirksamkeit des Vertrags nach § 135 Abs. 1 Nr. 2 GWB. § 134 Abs. 1 Satz 2 GWB bleibt unberührt.

VI.5.

Date of dispatch of this notice

06/09/2023