Wer ein Bauprojekt elektronisch ausschreibt, muss dafür Sorge tragen, dass kein Fremder die elektronische Datenübertragung manipulieren kann. FOTO DPA

Was es mit der elektronischen Kommunikation bei der E-Vergabe auf sich hat

Verschlüsseln oder signieren

Seit der Vergaberechtsreform im April dieses Jahres kommt der elektronischen Vergabe eine größere Bedeutung zu. Oberhalb der EU-Schwellenwerte ist die E-Vergabe und damit die digitale Kommunikation verpflichtend anzuwenden. „Für das Senden, Empfangen, Weiterleiten und Speichern von Daten in einem Vergabeverfahren verwenden die öffentlichen Auftraggeber und die Unternehmen grundsätzlich Geräte und Programme für die elektronische Datenübermittlung“, heißt es in den einschlägigen Paragrafen der anzuwendenden Vergabegesetze (§97 Abs. 5 des Gesetzes zu Modernisierung des Vergaberechts – VergRModG, §9 Abs. 1 der Vergabeverordnung – VgV beziehungsweise §11 EU VOB/A EU).

Hierzu gibt es einen „Stufenplan“. Dieser sieht vor, dass die Bekanntmachung bei der EU verpflichtend elektronisch vorzunehmen ist. Damit potenzielle Bieter die Vergabeunterlagen einsehen können, darf keine Registrierung verlangt werden. Die Vergabeunterlagen müssen barrierefrei herunterladbar sein.

Zu einem späteren Zeitpunkt muss die Kommunikation vollständig digital ablaufen. Dann dürfen Angebote nur noch in Ausnahmefällen in der heute üblichen Schriftform von der jeweiligen Vergabestelle entgegengenommen werden.

Das Vergaberecht sieht derzeit neben der schriftlichen auch die elektronische Angebotsabgabe vor. Hier nennt der Gesetzgeber folgende Schlagworte: „Verschlüsselung, fortgeschrittene Signatur, qualifizierte Signatur und – ganz neu – elektronische Angebotsabgabe in Textform“. Gerade letztere nimmt eine herausragende Stellung ein. Denn §53 Abs. 1 VgV und §11 EU VOB/A EU sehen die Angebote in Textform als Standard vor. Nur in begründeten Ausnahmefällen darf davon abgewichen werden und die elektronische Signatur vorgeschrieben werden (§53 Abs. 3 VgV; §11 EU Abs. 5 VOB/A EU: §13 EU Abs. 1.1 Satz 3 VOB/A EU).

Was bedeutet es, elektronische Daten digital zu signieren und zu verschlüsseln? Da elektronische Daten leicht manipuliert werden können, ist zum Beispiel der Urheber eines Dokuments nicht zweifelsfrei festzustellen. Auch innerhalb eines Dokuments können Veränderungen vorgenommen werden. Aus diesen Gründen war es lange Zeit undenkbar, sensible Daten elektronisch zu versenden.

Doch mit der elektronischen Signatur änderte sich das. Sie dient dazu, ein Dokument und einen Sender zu verifizieren. Das Dokument selbst bleibt ungeschützt, also „frei“ zugänglich lesbar. Wird das sogenannte Signatursiegel gebrochen, um etwa den Inhalt des Dokuments zu verändern, ist dies beim Öffnen und Prüfen der elektronischen Nachricht festzustellen. Jegliche Manipulation wird dadurch sofort ersichtlich.

Wozu dient nun die Überprüfung des Zertifikats? Bei der qualifizierten Signatur kann durch die Überprüfung der Inhaber der Signatur über ein Trust-Center ermittelt werden. Es werden keine persönlichen Daten angezeigt, sondern nur der Name der registrierten Person. Denn das Zertifikat ist personenbezogen.

Bei der fortgeschrittenen Signatur entscheidet der Sender, welche Daten bei der Prüfung angezeigt werden. Im Regelfall sind dies Name und Vorname des Senders.

Um Daten, die elektronisch übermittelt werden, für Dritte unlesbar zu machen, können sie verschlüsselt werden. Auf diese Weise wird das Dokument gesichert. Es kann dann nur noch vom Sender und vom Empfänger geöffnet und gelesen werden. Dazu wird der sogenannte öffentliche Schlüssel verwendet. Der „private“ Schlüssel bleibt verborgen auf dem Rechner, auf dem die Verschlüsselungssoftware installiert und das Schlüsselpaar generiert wurde.

Nachdem die Signatur mit der Verschlüsselung einhergeht, wird dieser Vorgang kaum unterschieden. Die fortgeschrittene Signatur wird normalerweise dafür verwendet, Daten zu sichern und zu verschlüsseln, um sie nicht unterschreiben zu müssen. Die fortgeschrittene Signatur ist ein reines Softwarezertifikat. Ein Lesegerät ist hierfür nicht nötig.

Die qualifizierte und damit zertifizierte Signatur ist nur mit einer Signaturkarte, einem passenden Lesegerät und der entsprechenden Software möglich. Die Zertifizierung und Verifizierung erfolgt durch ein Trust-Center. Sie hat eine Laufzeit von zwölf Monaten. Wenn die qualifizierte Signatur bei Vergaben eingesetzt werden soll, ist es wichtig, darauf zu achten, dass das Zertifikat am Tag der Angebotsöffnung gültig ist.

Die „elektronische Angebotsabgabe in Textform“ sieht keine digitale Signatur vor. Dennoch sollte das Angebot aber sicherheitshalber verschlüsselt werden.

Unter *www.staatsanzeiger-eservices.de* gibt es eine kostenfreie Software (GpG4Win). Mit ihr ist eine digitale Signatur (fortgeschrittene Signatur) und eine Verschlüsselung möglich. **> BSZ**

INFO Elektronische Schlüssel kopieren

Das Kopieren von elektronischen Schlüsseln auf ein anderes Gerät (Rechner) ist möglich, aber kompliziert. Vor allem, wenn nicht schon bei der Installation der entsprechenden Software daran gedacht wurde. Soll ein Dokument auf mehreren Rechnern geöffnet werden können, muss auf jedem Rechner die Software installiert, ein Schlüssel generiert werden und dem Dokument mitgegeben werden.

Wichtig für Vergabestellen:
Jeder „Verhandlungsleiter und Beisitzer“ (Vier-Augen-Prinzip) gibt mindestens zwei, besser mehrere öffentliche Schlüssel von den Rechnern in der Vergabestelle zur Öffnung der Angebote ab. Damit ist gewährleistet, dass auf mehreren Rechnern die Submission, also die Öffnung der Angebote, durchgeführt werden kann. Zu beachten ist, dass auf jedem Rechner mehrere Schlüssel für unterschiedliche Personen erzeugt werden können.

Lösung: Sicherung des elektronischen Schlüssels auf einem Security-USB-Datenstick.

INFO Unterschied zwischen digitaler Signatur und Verschlüsselung

Der Unterschied zwischen digitaler Signatur und Verschlüsselung lässt sich am besten beschreiben, wenn man eine Postkarte als Vergleich heranzieht.

Signatur – die Klarsichtfolie:
Ein Signieren der eigenen E-Mail bedeutet, dass man die E-Mail „abschließt“. Man setzt praktisch seine Unterschrift, um deutlich zu machen, dass man tatsächlich der Absender der Mail ist und versiegelt sie. Durch das Signieren der Mail schützt man sie davor, auf dem Weg durch das Netz von Dritten verändert zu werden. Beispielsweise könnte ein Angreifer die Mail zwischen zwei Kommunikationspartnern abfangen und den Inhalt nach Belieben verändern. Eine Signatur macht das unmöglich. Anschaulich könnte man sagen, dass man eine Postkarte weiterhin ganz normal und für jeden lesbar verschickt, sie aber in Klarsichtfolie einschweißt, sodass niemand mehr Änderungen vornehmen kann.

Verschlüsselung – der (bessere) Briefumschlag:
Eine Verschlüsselung ist noch mehr: Hier wird – anschaulich gesprochen – die Postkarte nicht mehr nur in Klarsichtfolie eingeschweißt, sondern in einen blickdichten Briefumschlag gesteckt und verschickt. Der Umschlag hat sogar noch die Eigenschaft, dass er nur von einer ganz bestimmten Person, nämlich dem Empfänger geöffnet werden kann. Damit ist die Kommunikation zwischen zwei Partnern gänzlich abgesichert und vertraulich.