Mag. iur. Dr. techn. Michael Sonntag

Signaturverordnung

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

© Michael Sonntag 2011

Inhalt

- Legt folgende Punkte fest
  - → Gebühren für die Aufsichtstätigkeit
  - → Anforderungen an ZDA
    - » Finanzielle Ausstattung
    - » Sicherheits- und Zertifizierungskonzept
  - → Prüfung von Komponenten und Verfahren
  - → Erforderliche Dienste bzw Anforderungen an Dienste
  - → Algorithmen und Parameter

Gebühren

- Sind Entgelt für die Tätigkeit der Aufsichtsbehörde
  - → Prüfung von Sicherheits-/Zertifizierungskonzept (≤ € 4.500)
    - » Und deren regelmäßige (jährliche) Prüfung (€ 1.500/3.000)
  - → Freiwillige Akkreditierung (€ 4.500)
  - → Anlassbezogene Prüfungen (€ 4.500)
  - → Erteilung von Auflagen wegen Mängeln, … (€ 700)
  - → Weiterführung des Widerrufsdienstes (€ 1/Zertifikat/Jahr)
    - » Bei Einstellung der Tätigkeit
    - » Sofern nicht jemand anderer (=anderer ZDA) dies übernimmt
- Achtung: Wird die Aufsichtsstelle (A-SIT) oder ein externer Gutachter benötigt, so kommen deren Gebühren dazu!
- Von gewissen Gebühren sind Gebietskörperschaften, Körp. öff. Rechts und Sozialversicherungen befreit
  - → Damit nicht der Staat an den Staat zahlt
- Jährlicher staatlicher Zuschuss von € 90.000-150.000

Anforderungen an ZDA: Finanzielle Ausstattung

- Anforderung aus der EU-Richtlinie: Ausreichende Finanzmittel für Arbeit und Haftungsrisiko, zB Versicherung
- Vorhandene Finanzmittel sind regelmäßig an die Aufsichtsstelle mitzuteilen
  - → Mindestkapital: € 300.000 Eigenmittel (eingezahlt!)
- Nachweis einer Haftpflichtversicherung
  - → Mindestens € 700.000, für mindestens 3 Fälle pro Jahr
- Ausnahme von diesen Verpflichtungen
  - → Bund, Länder, Gemeindeverbände und Gemeinden
  - → Körperschaften öff. Rechts (zB Kammern)
  - → Träger der Sozialversicherung
  - → Bei diesen geht man davon aus, dass sie genug Geld besitzen bzw sie können nicht (?) in Konkurs gehen!

Anforderungen an Signaturerstellungseinheiten

- Technische Komponenten müssen geprüft sein
- Rahmenbedingungen (Bitlänge etc.) müssen dem „Stand der Technik“ entsprechen
  - → Beliebte Aussage, immer problematisch! Praxis: Gutachten!
- Spezifik. für zu sign. Format muss allgemein verfügbar sein
  - → Daher „alte“ MS Office Dokumente → Niemals!
  - → Elemente, die dyn. Änderungen erlauben dürfen nicht verwendet werden (→ Praxisproblem: Wie ausschließen?)
- Signatur darf nur nach Autorisierung erfolgen
  - → PIN, Fingerabdruck, …
  - → Müssen sofort danach aus dem Speicher gelöscht werden
  - → Keine Eingabeerleichterungen bei wiederholter Eingabe
  - → Erfahren durch Dritte muss durch Gestaltung und Sperrmechanismen wirksam ausgeschlossen sein
    - » Wie sieht das etwa bei Fingerabdrücken aus?

Anforderungen an Zertifizierungsdienst

- Technische Einrichtungen von ZDAs sind von anderen Anwendungen und Funktionen zu trennen und eine Beeinflussung muss ausgeschlossen sein
  - → Problem: Virtualisierung = Trennung; Ausschluss der Beeinflussung nur möglich, wenn Performanz garantiert!
    - » Bei modernen Virtualisierungslösungen ist dies jedoch möglich
  - → Muss nicht nur für regulären Betrieb, sondern auch für Notfälle und außerhalb des Betriebs gelten
    - » „Außerhalb“ → Wartung, Reservegeräte, …
  - → Besondere Betriebssituationen sind zu dokumentieren
    - » Beispiel: Wartung, Gerätetausch (→ Sichere Löschung!), …
- Schutz vor unbefugtem Zutritt (=phys. Schutz)
- Schriftliche (oder dauerhafter Datenträger) Information
  - → Inhalt des Sicherheits- und Zertifizierungskonzepts
    - » Siehe später!

Personalausstattung

- Kein Personal mit Freiheitsstrafe für Vorsatztat >1 Jahr
  - → oder strafbare Handlung gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden/Beweiszeichen >3 Monate
  - → Was getilgt ist, zählt nicht mehr!
- Personal (zusammen, nicht jeder!) muss folgendes Wissen:
  - → Allg. EDV-Ausbildung, Sicherheitstechnologie, Kryptographie, el. Signaturen, PKI, techn. Normen (insb. Evaluierung), Hard- und Software
  - → Auf Aufforderung ist dies nachzuweisen, zB durch
    - » Absolvierung einer einschlägigen HTL, FH, Studium
    - » Facheinschlägige Tätigkeit von mindesten 3 Jahren

Sicherheits- und Zertifizierungskonzept

- Folgende Angaben sind als Minimum erforderlich:
  - → Name, Adresse, Niederlassungsstaat, Geschäftszeiten
  - → Art, Anwendungsbereich und Erbringung der Dienste
  - → Verfahren zur Antragstellung (insb. Identitätsprüfung!)
  - → Spezialinhalte: Pseudonym, Zusatzangaben, Vertretungsmacht
  - → Format und Erzeugung der Signaturerstellungsdaten
    - » Sowohl die der ZDA als auch der Signatoren
  - → Signaturprüfdaten (Zertifikat des ZDA)
  - → Eingesetzte Verfahren (Hashfunktionen …)
  - → Liste der eingesetzten, bereitgestellten und empfohlenen Signaturprodukte
  - → Sicherheit der Autorisierungscodes
  - → Gängige Dokumentenformate und Methoden zur Verhinderung dynamischer Veränderungen

Sicherheits- und Zertifizierungskonzept

- → Format und Gültigkeitsdauer der Zertifikate
- → Techn. Normen, Zugangsmodalitäten sowie Aktualisierungs- und Verfügbarkeitszeitraum der Verzeichnis-/Widerrufsdienste einschließlich des Sperrzeitraums
- → Nachvollziehbare und allgemein verständliche Methode zur sicheren Signaturprüfung
- → Format der Dokumentation von Sicherheitsvorkehrungen, Störfällen und bes. Betriebssituationen
  - » Unklar: Diese Dokumentation ist für Endkunden unzugänglich!
- → Schutz technischer Komponenten vor unbefugtem Zugriff
- → Schutz der Einrichtungen des ZDA vor unbefugtem Zutritt

- Konzept ist der Aufsichtsstelle in el. Form vorzulegen
  - → Muss mit el. Signatur des ZDA versehen sein
- Zusätzlich: Klar&allgemein verständliche Zusammenfassung

Zeitstempeldienste

- Verwendete Systeme und Produkte müssen „technisch und kryptographisch sicher“ sein
  - → Sehr allgemein; zumindest Verweis auf Stand der Technik, bestimmte Zertifizierungsverfahren etc. wäre hilfreich!
- Geprüfte Signaturerstellungseinheit erforderlich
- Nur Algorithmen/Parameter aus der VO sind erlaubt
- Zertifikate müssen ausschließlich hierfür dienen und diesen Verwendungszweck ausdrücklich bezeichnen
  - → Keine Verwendung von Zertifikate zur Zertifikatsausstellung
- Zeit: Mitteleuropäische Zeit mit Beachtung der Sommerzeit
  - → Andere Zeitzonen sind ausdrücklich anzugeben
    - » Aber diese nicht??? → SEHR schlecht!
  - → Abweichung darf höchstens eine Minute betragen

Prüfung von Komponenten und Verfahren

- Technische Aufgaben → Bestätigungsstelle
  - → In Österreich die einzige: A-SIT
- Bei der Prüfung von Komponenten und Verfahren sind Sicherheitsvorgaben der Bestätigungsstelle zu verwenden
  - → Insbesondere: Common Criteria (ISO 15408) oder ITSEC
- Aber: Werden techn. Komponeten und Verfahren in einer kontrollierten Umgebung eingesetzt, können techn. Sicherheitsanforderungen auch organisatorisch durch Personal oder durch Zugriffs-/Zutrittskontrollen erfüllt werden!
  - → Vorteil: Im ZDA-Rechenzentrum können auch unsichere Systeme verwendet werden, weil ohnehin keiner an sie herankommen kann (außer das vertrauenswürdige Personal)
  - → Ist durch die Bestätigungsstelle zu prüfen
- Besttätigung legt Bedingungen und Befristung (Zwang!) fest
  - → Unterlagen techn. Inhalts sind im Web zu veröffentlichen

Übersicht der ZDA in Österreich 15.4.2011

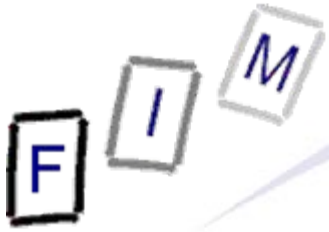
- A-Trust GmbH
  - → Auch: Bürgerkarte, Sachverständigenausweis, …
- Bundesamt für Eich- und Vermessungswesen
  - → Nur sicherer Zeitstempeldienst, keine Zertifikate!
    - » Preis ist gestaffelt; Rest verfällt zu Jahresende
      - – 100 Stück/Jahr → € 24 bis 500.000 Stück/Jahr → € 6.000,-
  - → http://www.bev.gv.at/qzsd
- Inaktiv:
  - → Datakom Austria GmbH
    - » Zertifikate übernommen von A-Trust GmbH
  - → Es existierten noch ein paar weitere, diese wurden inzwischen jedoch komplett eingestellt
- Quelle: http://www.signatur.rtr.at/currenttsl.pdf

Algorithmen

- Genaue Vorschrift, welche Kombinationen zulässig sind
  - → Signaturalgorithmus+Schlüsselerzeugung+Padding+Hash
- Signaturalgorithmen + Min. Schlüssellänge
  - → RSA ab 1024 Bit
  - → DSA ab 160 Bit
  - → Elliptische Kurven-DSA ab 160 Bit
- Hashfunktionen
  - → SHA-1
  - → RIPEMD160
  - → SHA-2: SHA-224, -256, 384, 512
  - → Whirlpool
- Padding (wenn Nachricht nicht exakt benötigte Länge hat)
  - → Sechs verschiedene
  - → Pseudo-Zufallszahlen (min. 64 Bit) erlaubt

Algorithmen

- Schlüsselgeneratoren
  - → Pseudo-Zufallszahlengenerator erlaubt
  - → Mindestens 80 Bit Entropie/Startwert
- Pseudozufallszahlengenerator:
  - → Müssen mit echten Zufallszahlen initialisiert werden
  - → Maximal 100 Signaturerstellungsdaten, dann erneute Initialisierung nötig
  - → Alternative (keine Begrenzung auf 100 Stück):
    - » Initialisierung mit echten Zufallszahlen
    - » 8 Bits pro Ausgabewert Anteil an echten Zufallszahlen
  - → Backups des Startwertes/interner Zustände sind verboten



Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

© Michael Sonntag 2011