erschienen in: Trust Center; Proceedings der Arbeitskonferenz Trust Center 95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 117-131

Mehrseitig sichere Schlüsselerzeugung

Hannes Federrath*, Anja Jerichow*, Andreas Pfitzmann*, Birgit Pfitzmann◊

*Technische Universität Dresden, Institut für Theoretische Informatik
{federrath, jerichow, pfitza}@inf.tu-dresden.de

◊Universität Hildesheim, Institut für Informatik
pfitzb@informatik.uni-hildesheim.de

Zusammenfassung

Wir untersuchen Möglichkeiten mehrseitig sicherer und vertrauenswürdiger Schlüsselerzeugung, also vertrauenswürdig für den individuellen Nutzer und seine Kommunikationspartner sowie bei Signierschlüsseln auch vertrauenswürdig für die staatlichen Regulierer von Kryptographie.

Zunächst werden für Signierschlüssel einige Verfahren diskutiert, wie Vertrauen für individuelle Nutzer und staatliche Regulierer von Kryptographie möglich wird. Diversitär generierte Schlüsselpaare könnten hierfür eine Lösung bieten. Unter bestimmten Voraussetzungen ist eine Erzeugung von Schlüsseln auch innerhalb der Geräte, die zum Signieren verwendet werden, denkbar. Die Anwendbarkeit von Fail-stop-Signaturverfahren wird diskutiert.

Die Problemerweiterung von digitalen Signaturen auf Datenverschlüsselung führt zu einem Schlüsselaustauschprotokoll, bei dem individuelle Teilnehmer nur minimales Vertrauen in dritte Instanzen setzen müssen.

1 Einführung

Im Zuge neuer Kommunikationsmöglichkeiten über digitale Netze besteht Bedarf für sichere, hier vor allem Integrität wahrende Dienste. Deren Implementation erfordert gewöhnlich technische und organisatorische Maßnahmen.

Ein notwendiges Hilfsmittel auf dem Weg zu sicheren Diensten ist Kryptographie. In der Vergangenheit wurden eine Reihe kryptographischer Verfahren entwickelt und untersucht, die den Anforderungen an sichere Kommunikation gerecht werden können. Digitale Signaturverfahren sind hierfür sehr bedeutungsvoll. Mit ihnen ist es möglich, digitale Dokumente gegen unerkannte nachträgliche Veränderungen durch jedermann zu schützen. Die digitale Signatur wird dokumentspezifisch vom Besitzer eines geheimen Schlüssels gebildet.

Einige staatliche Stellen der Bundesrepublik Deutschland prüfen derzeit, „ob unter bestimmten Voraussetzungen ‚elektronische Dokumente' mit ‚elektronischer Unterschrift' dem Schriftdokument rechtlich gleichgestellt werden sollen" [BMI_95]. Nach Verabschiedung entsprechender Gesetze wäre es demzufolge mit der digitalen Signatur möglich, Willenserklärungen abzugeben, die ebenso rechtswirksam sind wie Dokumente mit eigenhändiger Unterschrift.

Es besteht also die Forderung, die Funktionen der eigenhändigen Unterschrift auf digitale Signaturen abzubilden [Bize_92]:

1. Echtheitsfunktion — Es besteht Gewähr für das Herrühren der Willenserklärung vom Aussteller.
2. Identifikationsfunktion — Die Unterschrift macht die Identität des Ausstellers kenntlich, d.h. sie muß für ihn charakteristisch sein.
3. Abschlußfunktion — Die Unterschrift macht Abschluß bzw. Ende der Willenserklärung kenntlich, d.h. daß sie nicht mehr im Entwurfsstadium ist.
4. Warnfunktion — Der in Rechtsfragen unkundige Unterzeichner wird vor übereilter Unterschriftsgabe geschützt.
5. Beweisfunktion — Das in der Willenserklärung Vereinbarte ist für den später Beweispflichtigen leicht beweisbar.

Die zu verabschiedenden Vorschriften müssen darüber hinaus Regelungen zu den kryptographischen Verfahren, zu sicheren gerätetechnischen Umgebungen zum Signieren sowie zu Schlüsselerzeugung, -zertifizierung und -austausch enthalten.[1]

Über die neuen elektronischen Kommunikationsdienste sollen auch rechtlich relevante Dinge abgewickelt werden. Voraussetzung hierfür ist jedoch, daß alle Beteiligten, also viele Menschen, jeweils ein unterschiedliches Schlüsselpaar besitzen. Dem Teilproblem „sicherer Schlüsselaustausch“ kommt in öffentlichen Systemen[2] eine besondere Bedeutung zu, da Menschen miteinander kommunizieren werden, die keine Möglichkeiten haben, über einen Kanal außerhalb des Kommunikationsnetzes sicher Schlüssel auszutauschen. Deshalb werden am Kommunikationsprozeß Dritte beteiligt sein, die für die Partner vertrauenswürdig sein müssen. Über sie wird die notwendige Zertifizierung und Bereitstellung öffentlicher Schlüssel erfolgen.

Menschen haben unterschiedliche Sicherheitsbedürfnisse. Daher fordern wir zunächst, daß für die praktische Benutzung des Gesamtsystems kein unbedingtes oder gar hundertprozentiges Vertrauen in einen Dritten erforderlich ist. Eine gegenteilige Forderung wäre ebenso unrealistisch wie der Wunsch nach hundertprozentiger Sicherheit eines Systems.

Durch allgemeine Gewaltenteilung stellt der Staat die grundrechtlich gewährleistete Freiheit der Bürger sicher.[3] Deshalb sollte, wenn schon Vertrauen in Dritte notwendig ist, Gewaltenteilung möglich sein. So ist als ein Aspekt von Diversität nie Vertrauen in eine *einzige* Stelle nötig.

---

1 Dieses Papier behandelt nicht die sicheren gerätetechnischen Umgebungen zum Signieren. Es sei aber betont, daß sie keineswegs trivial sind; siehe z.B. die Simulationsstudien der Gruppe provet [BiHa_93, HaBi_93] oder manche Beispiele aus [Ande_94]. Einen Überblick über Verbesserungsmöglichkeiten gibt [PPSW_95].

2 d. h. Systeme ohne eingeschränkten Benutzerkreis

3 siehe z.B. [Aven_90, S.200], Stichw. Gewaltenteilung

Drei Maximen der Systemgestaltung lassen sich deshalb in folgender Weise formulieren:

1. So wenig wie möglich notwendiges Vertrauen in Dritte.
2. Diversität der Dritten, d.h. die Funktion der Dritten wird durch mehrere, vom Teilnehmer frei wählbare und unabhängige Instanzen geleistet.
3. Der Teilnehmer vertraut sich selbst.

Die folgenden Abschnitte diskutieren verschiedene Möglichkeiten mehrseitig sicherer Schlüsselerzeugung und -verteilung. Mehrseitig bedeutet hier vertrauenswürdig für den individuellen Nutzer sowie je nach Anwendung auch für seinen Kommunikationspartner und/oder für die staatlichen Regulierer von Kryptographie. In den Abschnitten 2 und 3 soll die Erzeugung von Signierschlüsseln im Vordergrund stehen. Abschnitt 4 beschreibt ein Schlüsselaustauschprotokoll für Konzelation, das nur minimales Vertrauen in Schlüsselverteilzentralen erfordert. Abschnitt 5 nennt technische und soziale Gründe, warum die rechtliche Regelung neuer Dienste in Kommunikationsnetzen sehr behutsam erfolgen sollte.

2 Erzeugung von Signierschlüsseln

Bei der Debatte über den Ort des Erzeugens geheimer Signierschlüssel (und damit natürlich auch öffentlicher Testschlüssel) treffen derzeit zwei kontroverse Standpunkte aufeinander.

Die staatlichen Regulierer von Sicherheit und Kryptographie meinen, sog. Trust Center seien geeignete Organisationen zur Schlüsselerzeugung. In Abschnitt 2.2 werden Gründe für diese Meinung genannt und kommentiert.

Dem Recht auf individuelle Selbstbestimmung und Selbstverantwortung[4] sowie der Privatautonomie des Menschen folgend besteht jedoch auch die Forderung, die Schlüsselerzeugung ausschließlich unter persönlicher und individueller Kontrolle eines Teilnehmers durchführen zu können.

Die aus den konträren Positionen entstehenden Interessenskonflikte werden im folgenden beleuchtet. Zunächst sollen jedoch einige für uns wesentliche Aspekte zu Trust Centern herausgearbeitet werden.

2.1 Trust Center

Unter dem Begriff Trust Center sollten zunächst die Funktionen von zentralen Einrichtungen (Dritten) zur Schlüsselzertifizierung und -verteilung verstanden werden. In diese Dritten (bezogen auf zwei Kommunikationspartner) ist Vertrauen notwendig, damit eine Teilnahme am Verfahren möglich ist. Oft werden sie auch als „vertrauenswürdige“ Dritte bezeichnet. Dieses Begriffsverständnis verschleiert, daß auch die Trust Center fehlerhaft sein können. Für die Konsequenzen aus Fehlern sind sie jedoch verantwortlich. Da der Begriff Trust Center eine unfehlbare Bastion an Vertrauen vorspiegelt, die wir so nicht sehen, verwenden wir den

4 siehe z.B. [Aven_90, S.346], Stichw. Persönlichkeitsrecht

Begriff Trust Center nicht und orientieren uns begrifflich jeweils an der funktionalen Bedeutung (Zertifizierungsstelle, Schlüsselverteilzentrale, Zentralen) des Dritten im Gesamtsystem.

Für die praktische Verwendbarkeit von digitalen Signaturen unter gesetzlich geregelten Bedingungen sind Einrichtungen zur Zertifizierung öffentlicher Testschlüssel, sog. Zertifizierungsstellen, notwendig. Ihrer meist hierarchischen Anordnung entsprechend ist die zu einem zertifizierten Schlüssel gehörende Zertifikatskette eine Garantie dafür, Verantwortlichkeiten im Streitfall exakt zuordnen zu können. Deshalb gehört die gesamte Zertifikatskette unseres Erachtens stets zur Signatur (vgl. [Hamm_95]).

Da das Vertrauen in ein Zertifikat nur so groß sein kann wie das Vertrauen in den Ausstellenden, muß dieser für die Kommunikationspartner vertrauenswürdig sein. Der Forderung nach minimalem Vertrauen in Dritte folgend, muß die Vertrauenswürdigkeit bzw. korrekte Arbeitsweise von Zertifizierungsstellen unbedingt überprüfbar sein.

Beim *Zertifizierungsprozeß* sollte folgendes geschehen: Ein Teilnehmer X unterschreibt mit seiner eigenhändigen Unterschrift seinen öffentlichen Testschlüssel $\ddot{o}_X$. Er erklärt damit, daß alle Signaturen, die mit diesem $\ddot{o}_X$ als korrekt erkannt werden, von ihm geleistet wurden. Die Zertifizierungsstelle ihrerseits signiert mit ihrem geheimen Signierschlüssel den öffentlichen Testschlüssel $\ddot{o}_X$ des Teilnehmers X und bestätigt damit die Authentizität von $\ddot{o}_X$.

Da eigenhändige Unterschriften nicht sehr schwer zu fälschen sind, sollte die Unterschrift von X zusätzlich notariell beglaubigt sein, und zwar von einem Notar, der von der gewählten Zertifizierungsstelle unabhängig ist.

Bei *Test eines Zertifikats* kann jeder Teilnehmer die Signatur der Zertifizierungsstelle unter $\ddot{o}_X$ prüfen, indem die Signatur mit dem öffentlichen Testschlüssel der Zertifizierungsstelle auf Korrektheit getestet wird. Damit die Authentizität des öffentlichen Testschlüssels der Zertifizierungsstelle gewährleistet ist, muß dieser ebenfalls durch eine vertrauenswürdige Stelle zertifiziert sein. Durch rekursive Zertifizierung der öffentlichen Schlüssel bildet sich so eine Zertifikatskette.

Randbedingungen für die Zurechenbarkeit von geleisteten Signaturen sind zunächst:

- Die Zertifikatskette ist sicher, d.h. alle öffentlichen Schlüssel sind authentisch. Hierfür sind alle beteiligten Zertifizierungsstellen verantwortlich.
- Für unerlaubt zertifizierte Schlüssel haftet die Zertifizierungsstelle.
- Die verwendeten Geräte sind sicher. Das bedeutet hier:
  - Funktionieren der Endgeräte[5], z.B. es wird tatsächlich das signiert, was angezeigt wird.
  - Sicheres Erzeugen und Aufbewahren der Schlüssel. Hierfür ist ebenfalls der Nutzer verantwortlich.
- Die verwendeten kryptographischen Mechanismen sind sicher, d.h. nicht brechbar. Hierfür kann niemand unmittelbar verantwortlich sein, da die kryptographischen Mechanismen von unbewiesenen komplexitätstheoretischen Annahmen ausgehen.

---

5 siehe hierzu auch die Bemerkungen in Abschnitt 2.3

Für rechtlich relevante Kommunikation, in die Zentralen z.B. durch Schlüsselzertifizierung oder -verteilung involviert sind, stellt sich die Frage, für wen sie vertrauenswürdig sein müssen. Das sind die Kommunikationspartner selbst, aber auch die Schiedsinstanzen im Falle eines Rechtsstreits. Dies unterstreicht den Mehrseitigkeitsaspekt von Sicherheit. Um mehrseitiges Vertrauen in die Trust Center zu erreichen, müßten also alle Seiten in ihren Zulassungs- und Kontrollprozeß integriert sein. In der Praxis wird das schwer möglich sein.

Die Schiedsinstanzen im Falle eines Rechtsstreits werden i.d.R. staatliche Stellen sein. Ebenso werden staatliche Stellen über die Zulassung von Trust Centern entscheiden oder selbst welche betreiben. Ist einer der beiden Kommunikationspartner dann gleichzeitig eine staatliche Stelle, so ergibt sich unversehens eine Macht- und Kompetenzkonzentration, die dem Mehrseitigkeitsaspekt von Sicherheit aus der Sicht des anderen Kommunikationspartners schaden könnte.

Um dem präventiv entgegenzutreten, bedarf es unseres Erachtens einer strikten Trennung unterschiedlicher Aufgaben- und Verantwortungsbereiche innerhalb des Staates und klarer, für jeden Bürger einsehbarer und nachvollziehbarer Regeln zur Zulassung, zum Betreiben und zur Kontrolle von Trust Centern.

2.2 Alleinige Erzeugung von Signierschlüsseln in Zentralen

Da Zentralen zwangsläufig mit Schlüsseln zu tun haben werden, wird häufig vorgeschlagen, z.B. von den staatlichen Regulierern von Kryptographie, sie gleich auch für die Schlüsselerzeugung einzusetzen.

Es sollen die öffentlichen Testschlüssel und die geheimen Signierschlüssel zentral generiert werden. Die öffentlichen Testschlüssel sollen danach durch die Zentrale zertifiziert werden. Die geheimen Signierschlüssel werden in der Zentrale direkt auf Geräte gebracht. Schließlich sollen die Signierschlüssel an allen Orten, an denen sie technisch bedingt zwischengespeichert wurden, gelöscht werden.

Als Argumente für diese Art der Schlüsselerzeugung werden u.a. die folgenden Punkte genannt, die kommentiert werden sollen:

1. Eine Diskreditierung des Systems soll von vornherein ausgeschlossen werden. Dabei ist gemeint, daß Benutzer durch falsche Schlüsselerzeugung Möglichkeiten zur Fälschung erzeugen und die Berichterstattung das digitale Signieren als Ganzes in Verruf bringen könnten.

   Kommentar: Zum einen würden die meisten Benutzer die Schlüssel mit nicht selbst programmierten Algorithmen erzeugen; Zertifizierung dieser Algorithmen würde also die Gefahr wesentlich senken. Für das Restproblem gilt unseres Erachtens dasselbe wie unter 2. Da zudem, wie auch dieses Papier zeigen soll, die alleinige Erzeugung in Zentralen strittig ist, könnte diese Variante bereits „in üblem Ruf *sein*“, bevor ihre Vorteile gegenüber anderen Varianten zum Tragen kommen.

2. Ein Nutzer kann, da er seinen eigenen geheimen Schlüssel nie selbst erfahren kann, ihn nicht „herumerzählen“. Ein Angreifer kann ihn beim Nutzer nicht aushorchen.

Kommentar: Im positiven Sinn bedeutet dies, daß der Staat „fürsorglich“ zu seinen Bürgern ist, jedoch wird sich der mündige Bürger nicht mit dieser aufgezwungenen Fürsorglichkeit zufriedengeben. Darüber hinaus setzt dieses Argument das Vertrauen in die physische Sicherheit des Signiergerätes voraus (vgl. [PPSW_95]).

Auch liegt bei eigenhändigen Unterschriften eine solche Fürsorge nicht vor: Man kann blanko signiertes Papier verteilen (Herumerzählen des geheimen Schlüssels) oder eine so vereinfachte Unterschrift verwenden, daß sie leicht nachzuahmen ist (schlechte Schlüsselwahl).

3. Die sichere Schlüsselerzeugung in privaten Geräten, etwa Personal Computer und Personal Digital Assistants, ist ungeeignet, da evtl. durch Viren oder Trojanische Pferde gefährdet.

   Kommentar: Auch hier spielt offenbar die Fürsorglichkeit des Staates eine Rolle. Gleichzeitig wird aber übersehen, daß der ordnungsgemäße Ablauf der Schlüsselerzeugung, speziell das ordnungsgemäße Löschen des in der Zentrale zwischengespeicherten geheimen Signierschlüssels, für den Nutzer schwer oder nicht überprüfbar ist. Darüber hinaus existieren bis heute keine tauglichen Evaluierungswerkzeuge, mit denen zweifelsfrei festgestellt werden kann, daß die technischen Systeme, z.B. die verwendeten Betriebssysteme, in der Zentrale die Schlüsselerzeugung im o.g. Sinne korrekt ausführen. Das bedeutet beispielsweise, daß das Vorhandensein verdeckter Kanäle in den Zentralen und aus den Zentralen heraus nie sicher ausgeschlossen ist.

   Auf das Argument, wie man überhaupt zertifizieren wolle, wenn man der Sicherheit von Betriebssystemen nicht vertraut, kann man entgegnen, daß ein reines Zertifizierungsbetriebssystem nicht zwingend größer und komplexer sein muß als das des Benutzerendgerätes, aber es muß auf jeden Fall evaluiert werden.

4. Zentrale Schlüsselerzeugung ist als Verlusttoleranzmaßnahme besser geeignet als andere Verfahren.

   Kommentar: Dieses Argument hat verschiedene Aspekte. *a)* Im Falle eines Verlustes des geheimen Schlüssels kann dem Nutzer geholfen werden. Es wäre möglich, daß dem Nutzer erneut derselbe Schlüssel generiert werden kann. Das ist dann jedoch technisch gleichbedeutend mit einer Verletzung der Forderung nach Löschen des in der Zentrale zwischengespeicherten geheimen Schlüssels. *b)* Im Falle der Sperrung wegen zu häufiger Fehleingabe oder des Verlustes der Zugangsberechtigung, z.B. PIN, zum Signieralgorithmus mit dem geheimen Schlüssel kann die Sperre durch Dritte aufgehoben werden. Hierfür ist es aber sinnvoller, nur ein Master-Paßwort zur Aufhebung der Sperre zu speichern. Hiermit ist nur dann Mißbrauch möglich, wenn man sich zugleich Zugang zum Gerät des Benutzers verschafft.

5. Man muß den Zentralen sowieso vertrauen, warum also nicht auch hier.

   Kommentar: Für einen Angriff auf die Schlüsselerzeugung genügen i.d.R. passive, „abhörende“ Angriffe. Für Angriffe auf die Schlüsselzertifizierung sind jedoch aktive, „verändernde“ Angriffe erforderlich. Passive Angriffe sind meist einfacher durchzuführen als aktive und zudem praktisch nicht erkennbar. Insbesondere geht die in Abschnitt 2.1 genannte Möglichkeit, Verantwortung für Schlüssel zuzurechnen, verloren, wenn der geheime Schlüssel auch in der Zentrale bekannt war.

Auch ist wegen der unter 3. angesprochenen Schwierigkeit mit der Sicherheit des Betriebssystems der Zentrale gegen Insider eine Minimierung der kritischen Funktionalität wichtig.

Offenbar sind die genannten Argumente für eine zentrale Schlüsselerzeugung nur teilweise tragend. Unterstellt man, daß es andere Verfahren gibt, die den Anforderungen an die Signaturschlüsselerzeugung besser gerecht werden als die alleinige Erzeugung in Zentralen, sind nur Spekulationen darüber möglich, ob weitere, nicht genannte Ziele verfolgt werden sollen.

Eine Variante des hier vorgestellten Verfahrens ist die Erzeugung von Teilen der verschiedenen Schlüssel in unterschiedlichen Zentralen. Die dadurch erreichbare Sicherheitssteigerung ist zunächst organisatorischer Ausprägung. Durch technisch unterschiedliche Zentralen, etwa von verschiedenen Herstellern, ist auch Diversität der Funktionsrealisierung gegeben. Damit lassen sich evtl. Angriffe über verdeckte Kanäle und Trojanische Pferde erschweren, da jetzt *alle* beteiligten Zentralen abgehört werden müssen.

Eine Mindestanforderung für die alleinige Erzeugung der Schlüssel in Zentralen ist also deren Erzeugung in mehreren diversitären Zentralen, da jetzt alle Zentralen zusammenarbeiten müssen, um den Signaturschlüssel zu erfahren.

Wir halten die alleinige Signierschlüsselerzeugung in Zentralen für nicht geeignet, da sie unserer Forderung nach minimalem Vertrauen in dritte Instanzen widerspricht. Selbst bei alleiniger Erzeugung in mehreren diversitären Trust Centern muß, damit ein Vertrauen in die Schlüsselerzeugung noch möglich ist, mindestens einer fremden Instanz getraut werden. Dies ist für uns jedoch schon zuviel Vertrauen.

2.3 Alleinige Erzeugung von Signierschlüsseln unter Kontrolle des Nutzers

Die Möglichkeit, geheime Signaturschlüssel ausschließlich unter persönlicher Kontrolle eines Nutzers zu erzeugen und den zugehörigen öffentlichen Testschlüssel nachher zertifiziert zu bekommen, sollte deshalb niemandem verwehrt werden. Gleichzeitig gibt es weder technische noch juristische[6] Gründe, warum die Autonomie des Teilnehmers bei der Signierschlüsselerzeugung aufgegeben werden sollte. Von den staatlichen Stellen (bzw. deren Vertretern) wird gleichermaßen bestätigt, daß es keine Situation gibt, wo sie zur Erfüllung ihrer Aufgaben in Kenntnis des Signierschlüssels kommen müssen. Außerdem sollte jeder Mensch seine privatrechtlichen Geschäftsbeziehungen möglichst weitgehend so gestalten können, wie er es für richtig hält.[7]

Da der Nutzer jetzt nur sich selbst und der selbst gewählten Technik vertrauen muß, ist auch er für die Güte des Schlüsselerzeugungsprozesses verantwortlich. Natürlich kann der Nutzer

6 z.B. Verbrechensbekämpfung

7 siehe z.B. [Aven_90, S.362], Stichw. Privatautonomie

selten Schlüssel ganz allein erzeugen und auf Geräten unterbringen.[8] Er benötigt einen oder mehrere „Helfer“, z.B. Hersteller und Programmierer des Schlüsselgenerieralgorithmus. Um dem „Helfer“ (bzw. seiner angebotenen Technik) trauen zu können, sind selbstverständlich klare Zulassungsregeln und -prüfungen notwendig. Leider ist auch hier nie ganz auszuschließen, daß der „Helfer“ nur ein getarnter Angreifer ist. Insbesondere die organisatorische Komplexität des Gesamtprozesses Schlüsselerzeugung dürfte jedoch kleiner sein als bei zentraler Erzeugung. Durch die hinzukommende Diversität über verschiedene Anbieter und Hersteller entsprechender Ausrüstungen ist eine Diskreditierung des Gesamtsystems nicht wahrscheinlich.

Wir wollen betonen: Schlüsselerzeugung unter individueller Kontrolle des Nutzers löst nicht alle Probleme[9] und birgt evtl. andere Risiken[10]. Es gibt jedoch keinen wirklichen Grund, einer Person die individuelle Schlüsselerzeugung zu verwehren.

Ein praktisch verfügbares System, das mit nutzererzeugten Schlüsseln arbeitet, ist das von dem Amerikaner Philip Zimmermann 1990 realisierte Konzept „Pretty Good Privacy (PGP). Public Key Encryption for the Masses“. Die „Zertifizierung“ von Schlüsseln erfolgt dezentral durch die Benutzer des Systems. Da die mit privater Zertifizierung verbundenen Haftungskonsequenzen juristisch unklar sind und generell wohl nur schwer geregelt werden können, ist dieses System für rechtsverbindliche Telekooperation weniger geeignet, wohl aber für gesicherte Kommunikation außerhalb juristischer Bindungen.

3 Die goldene Synthese – Vorschläge und Lösungsmöglichkeiten

Damit in absehbarer Zeit öffentliche rechtsverbindliche Kommunikation mittels digitaler Signaturen möglich wird, muß ein für alle Seiten akzeptabler Weg der Schlüsselerzeugung gefunden werden.

Hierfür sind sicherlich Kompromisse nötig. Daher schlagen wir eine Synthese der Standpunkte

- alleinige Erzeugung in Zentralen und
- alleinige Erzeugung unter Kontrolle der Teilnehmer

vor. Schlüsselerzeugung soll also unter Beteiligung sowohl von Zentralen als auch des Nutzers so erfolgen, daß die Sicherheit des Gesamtsystems nur verletzt werden kann, wenn alle Parteien bzw. ihre Rechner sich falsch verhalten.

Diese Synthese unterstreicht nochmals den Mehrseitigkeitsaspekt von Sicherheit.

---

8 Es sei denn, er kann diese Geräte selbst herstellen, Schnittstellen selbst programmieren, u.s.w. Das gilt offenbar für die meisten Menschen nicht. Selbst Fachleute stellen i. allg. nicht als Einzelne vollständige Geräte her.

9 Beispielsweise die Konstruktion eines (ausforschungs)sicheren Endgeräts.

10 Beispielsweise die Unsicherheit des Nutzers über tatsächlich erfolgtes Löschen des im TC zwischengespeicherten geheimen Schlüssels gegenüber erhöhter Gefahr von Viren oder Trojanischen Pferden im Personal Computer zu Hause.

Im folgenden wollen wir auf technische Lösungsmöglichkeiten der Synthese eingehen.

3.1 Diversitär generierte Schlüsselpaare

Die Grundidee diversitär generierter Schlüsselpaare soll am Beispiel von zwei je Nutzer erzeugten Schlüsselpaaren demonstriert werden:

- 1 Paar wird in einer Zentrale Z erzeugt:

  $ö_z$, g_z (öffentlicher und geheimer Z-Schlüssel)

- 1 Paar wird unter Kontrolle (Autonomie) des Nutzers A erzeugt:

  $ö_a$, g_a (öffentlicher und geheimer A-Schlüssel)

Zum Signieren eines Dokuments unterschreibt der Nutzer jetzt stets mit beiden Signierschlüsseln, d.h. dem geheimen Z-Schlüssel g_z und dem geheimen A-Schlüssel g_a:

Sei m ein digitales Dokument (Bitkette). Sei $hash(x)$ eine kollisionsfreie Hash-Funktion.

1. Bilde den Hash-Wert h des Dokumentes: $h = hash(m)$
2. Bilde die Signatur s des Dokumentes: $s = g_z(h) \mid g_a(h)$

Das Zeichen „|“ bedeutet, daß die beiden getrennt berechneten Teile $g_z(h)$ und $g_a(h)$ der Signatur s aneinandergehängt werden.

Die auf diese Weise gebildeten Signaturen können parallel geleistet und geprüft werden. Der Mehraufwand dieses Verfahrens dürfte damit kleiner als Faktor 2 sein, da die Hash-Funktion nur einmal berechnet werden muß. Eine mögliche technische Lösung ist, zwei separate Geräte zu verwenden. Eines stammt vom Nutzer und enthält dessen Schlüssel. In dieses Gerät ist dann ein Gerät der Zentrale, z.B. ein Chip, einsteckbar. Beispielsweise bei Mobiltelefonen werden solche Einsteck-Chips verwendet.

Verallgemeinert man das beschriebene Vorgehen, so besitzt der Nutzer beliebig viele diversitäre Schlüssel. Für verschiedene Anwendungs- und Sicherheitsbereiche wären dann unterschiedliche (Mindest)-Diversitätsgrade vorgeschrieben. Der Nutzer erzeugt sich also mindestens einen A-Schlüssel und erhält je nach Diversitätsgrad mehrere Z-Schlüssel.

Als Folge der Diversitätseigenschaft des Schlüssels benötigen die Zertifizierungshierarchien Informationen darüber, wieviele Schlüssel ein Nutzer besitzt, denn nur die Verwendung *aller* gültigen (erforderlichen) Schlüssel bildet eine gültige Signatur. Sollte das Testen einer Signatur negativ enden, gibt es verschiedene Möglichkeiten der Fehlermeldung. Die Meldung „Signatur falsch!“ läßt sich auch detaillierter ausdrücken, z.B. „Signatur mit Z-Schlüssel falsch! Signatur mit A-Schlüssel richtig.“

Der entscheidende Punkt dieses Verfahrens ist, daß die jeweiligen Verantwortungsträger (Staat für Zentrale, Teilnehmer für sich selbst) entscheiden können, ob die Einbeziehung „ihres“ Schlüsselteils in die Signatur erfolgen soll.

3.2 Signierschlüsselerzeugung innerhalb des Signiergerätes

Bestehen die technischen Möglichkeiten, so kann jedes einzelne Endgerät, mit dem signiert werden soll, auch selbst ein Schlüsselpaar für die digitale Signatur generieren. Voraussetzung ist hier, daß es vertrauenswürdig ist für den Nutzer und den Regulierer. Diese Voraussetzung besteht aber generell, wenn Regulierer wünschen, daß die Benutzer ihre geheimen Schlüssel nicht kennen.

Technisch sind die algorithmischen Aspekte der Schlüsselerzeugung kein Problem. Bei derzeit üblichen Signaturverfahren braucht man hierfür dieselben Grundtechniken wie für das Signieren. Kryptokoprozessoren sind hierfür bestens geeignet. Natürlich dauert die Schlüsselerzeugung etwas länger als das Signieren. Will man Speicherplatz sparen, kann der Code nach einmaligem Gebrauch gelöscht werden. Beispielsweise das System nach [BBCM_94] hat Schlüsselerzeugung auf dem Chip.

Jeder Schlüsselerzeugungsprozeß muß mit etwas Zufälligem beginnen. Falls ein idealer Zufallszahlengenerator auf dem Gerät nicht implementierbar ist, erwartet das Gerät „zufällige“ Eingaben von außen, d.h. wegen der mehrseitigen Sicherheit vom Regulierer[11] und vom Nutzer[12]. Bei interner EXOR-Verknüpfung dieser Zufallsanteile ist die resultierende Zufallszahl mindestens so zufällig und geheim wie der beste ihrer Teile, und somit auch der geheime Schlüssel.

Um sicherzustellen, daß die Nutzereingaben von niemandem abgehört werden können, sollte deren Eingabe außerhalb der Zentrale und mit selbst gewählten Hilfsmitteln erfolgen. Um zu garantieren, daß die Anteile von den richtigen Parteien kommen, muß das Gerät (dem beide vertrauen) jeweils anzeigen, daß es diesen Zufallsanteil akzeptiert. Andernfalls verweigert der Regulierer das Zertifikat bzw. der Nutzer die Nutzung des Geräts.

Die Erzeugung von Signierschlüsseln in sehr kleinen Endgeräten ist sicherlich bisher ungebräuchlich, jedoch sind bereits viele Krypochips verfügbar, die dies leisten. Außerdem ist Signieren mit kleinen Geräten ohne Anzeige stets problematisch und daher ungebräuchlich, da es weitere Anriffspunkte bietet.[13]

Die durch diesen Vorschlag erfolgte Zuspitzung des Problems „Wie baue ich ein vertrauenswürdiges Endgerät?“ scheint momentan noch ungelöst (siehe auch [PPSW_95]). Dieses Problem muß aber in *jedem Fall* gelöst werden, wenn mit einem technischen Gerät eine sichere Signatur geleistet werden soll.

3.3 Anwendungsmöglichkeit von Fail-stop-Signaturen

Fail-stop-Signaturen [PfWa_91] sind im Rahmen dieses Papiers als Maßnahme gegen Diskreditierung des Signatursystems von Interesse.

---

11 Um den Interessen des Regulierers gerecht zu werden.

12 Um dem Autonomieinteresse des Nutzers gerecht zu werden.

13 Z.B.: Das extern, d.h. außerhalb des Signiergerätes angezeigte Dokument ist nicht das, welches mit dem Gerät signiert wird.

Der Begriff „Fail-stop“ besagt allgemein, daß, sofern etwas schiefgeht, sich dies unbestreitbar herausstellt. Danach kann das Verfahren gestoppt werden. Er ist angelehnt an das bekanntere „Fail-safe“ (Ausfälle in einen sicheren Zustand). „Fail-safe“ sind z.B. Eisenbahnsignale, die bei Durchtrennung der Steuerdrähte in die Stop-Position hinunterklappen. Fail-stop-Signaturen sind nun Signaturen mit einer Fail-stop-Eigenschaft bzgl. der Sicherheit des kryptographischen Verfahrens.[14] Genauer: Wenn ein Fälscher das kryptographische Verfahren bricht, z.B. unerwartet große Zahlen faktorisieren kann oder Kollisionen der Hashfunktion findet und damit Signaturen fälscht, so kann der behauptete Signierer einen sogenannten Fälschungsbeweis erzeugen, anhand dessen jeder sehen kann, daß das Verfahren gebrochen ist. Ein Beispiel wäre, daß der Signierer explizit die Kollision der Hashfunktion vorlegen kann.

Dadurch kann ein Benutzer das Verfahren nicht diskreditieren, denn *ohne* Fälschungsbeweis kann er nicht behaupten, es sei gebrochen. Insbesondere entsteht kein Fälschungsbeweis, wenn der Benutzer seinen geheimen Schlüssel herumerzählt hat, denn damit erzeugte Signaturen sind im kryptographischen Sinne keine Fälschungen. In gleicher Weise unterscheidet man, wenn die Benutzergeräte manipulationsgeschützt sind, ein Versagen dieses Schutzes vom Brechen des kryptographischen Verfahrens. (Man unterscheidet natürlich nicht echte Signaturen von solchen, die auf Diebstahl des Schlüssels bzw. Diebstahl des Endgerätes und Brechen seines Manipulationsschutzes oder Ausspähen der PIN beruhen.)

Technisch benötigen Fail-stop-Signaturen einen sogenannten Vorschlüssel, der nicht vom Signierer selbst gewählt wird. Zum Beispiel kann das eine große Zahl sein, deren Faktoren später als Fälschungsbeweis gelten würden.[15] Bei der Erzeugung dieses Vorschlüssels können die Zentralen wieder nützlich werden. Der Erzeugung müssen alle Personen vertrauen, die einen Nachteil hätten, wenn durch falsche Wahl des Vorschlüssels fälschlich der Eindruck entstünde, das kryptographische Verfahren sei gebrochen. Wir nennen sie Risikoträger. Einer davon ist der Staat, wenn er keine Diskreditierung des Verfahrens wünscht. Ob es weitere gibt, hängt von der Anwendung ab, insbesondere der juristischen Entscheidung, wer nach einem Fälschungsbeweis für Konsequenzen der als gefälscht bewiesenen Signaturen haften soll. Sind die Risiken nur finanziell, kann eine einzelne Zentrale den Vorschlüssel erzeugen und dafür haften.

Mehrseitig sichere Vorschlüsselerzeugung, d.h. ein Protokoll, das nur gebrochen werden kann, wenn alle beteiligten Parteien betrügen, ist im Prinzip für alle Fail-stop-Signatursysteme möglich [PfWa_90]. Dies kann man zunächst für Diversität zwischen mehreren Zentralen einsetzen. Besonders effizient geht gemeinsame Vorschlüsselerzeugung für das Fail-stop-Signatursystem aus [HePe_93], das sowieso derzeit das effizienteste ist (siehe [PePf_95] für mehr Einzelheiten). Es beruht auf der Schwierigkeit, diskrete Logarithmen zu berechnen. Als Vorschlüssel ist hier letztlich einfach eine Zufallszahl zu

---

14 Analog könnte man von Fail-stop-Trust-Centern sprechen, wenn jede Durchbrechung der Sicherheit ihrer Organisation und Betriebssysteme erkannt und von Fehlern auf Benutzerseite unterschieden werden kann. Dies wird gerade durch das in Abschnitt 2.1 beschriebene Verfahren zur Verantwortungszuweisung erreicht.

15 In [DaPP_94] gibt es eine Konstruktion aus einer beliebigen Hashfunktion, die bei Einsetzen einer schlüssellosen Hashfunktion zu einem Fail-stop-Signatursystem ohne Vorschlüssel führt. Unterschriften und geheime Schlüssel sind aber wesentlich länger als bei anderen Verfahren.

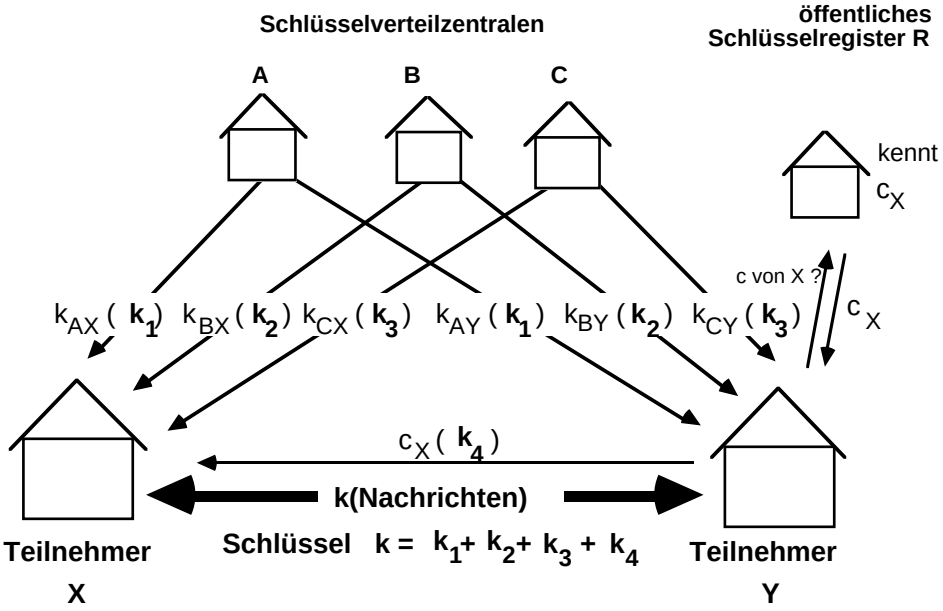
erzeugen (während bei obigem Beispiel mit Faktorisierung der Vorschlüssel zwei große, geheime Primfaktoren haben soll, was gemeinsame Erzeugung erschwert). Das einfachste wäre, daß man sich darauf einigt, alte Zufallszahltabellen der RAND-Corporation in einer kanonischen Weise zu benutzen. Eine Zentrale kann den daraus resultierenden Vorschlüssel bekanntgeben und jeder kann sie auf Wunsch nachprüfen. Der Vorschlüssel kann allen Signierern gemeinsam sein.

Es sei allerdings nicht verschwiegen, daß Fail-stop-Signatursysteme einen gewissen Preis fordern. Erstens sind die Signaturen bei allen bisherigen Systemen nicht ganz so kurz wie bei üblichen Signatursystemen. Zweitens wird pro Signatur eine gewisse Anzahl echt zufälliger Bits benötigt. Drittens müssen signierte Nachrichten aufgehoben werden, um sie ggf. mit einer Fälschung vergleichen zu können.

4 Schlüsselaustausch bei Konzelation

Die bisherigen Bemerkungen bezogen sich fast ausschließlich auf digitale Signaturen, also Probleme der Integrität von Daten. Sicherheit umfaßt aber auch Vertraulichkeit von Daten. Ein Teil von Vertraulichkeit ist die Datenverschlüsselung (Konzelation). Für Konzelation kommen aus Effizienzgründen meist symmetrische oder hybride Verschlüsselungsverfahren zum Einsatz.

Das folgende Verfahren beschreibt beispielhaft, wie Schlüsselaustausch für Konzelation mit möglichst wenig Vertrauen in dritte Instanzen, z.B. Schlüsselverteilzentralen, erfolgen kann.[16]



Schlüsselaustausch bei Konzelation

16 Um die Verfügbarkeit des Schlüsselverteilprotokolls zu gewährleisten, sind noch Authentikationsprobleme zu lösen, die hier nicht behandelt werden.

Zwei Teilnehmer X und Y, die sich noch nie zuvor getroffen haben, sollen einen zufälligen Schlüssel erhalten, um vertraulich miteinander kommunizieren zu können. Ein Angreifer soll passive Mithilfe aller beteiligten Schlüsselverteilzentralen haben und kann alle Kommunikation im Netz abhören.

Die Abbildung demonstriert den Schlüsselaustausch sowie das Verschlüsseln einer Nachricht.

Die Teilnehmer X und Y haben mit den Schlüsselverteilzentralen A, B und C Schlüssel (k_{AX}, k_{BX}, k_{CX}, k_{AY}, k_{BY}, k_{CY}) ausgetauscht. In der Abbildung sind das symmetrische Schlüssel.

X und Y erhalten über die Schlüsselverteilzentralen in verschlüsselter Form die Teile k_1, k_2 und k_3 des Schlüssels k, den sie zur Konzelation verwenden wollen.

Ein Teilnehmer, hier Y, sendet dann dem anderen, also X, noch einen weiteren Schlüssel (k_4) des symmetrischen Konzelationssystems, den er mit dem ihm bekannten öffentlichen Schlüssel c_X des Partners konzeliert.

Beide Partner verwenden als symmetrischen Konzelationsschlüssel die Summe k aller ihnen im symmetrischen Schlüsselverteilprotokoll mitgeteilten Schlüssel k_1, k_2 und k_3 und des zusätzlichen Schlüssels k_4. Um diese Summe $k=k_1+k_2+k_3+k_4$ zu erhalten, muß ein Angreifer alle Summanden erfahren, d.h. die passive Mithilfe aller Schlüsselverteilzentralen haben *und* das asymmetrische Konzelationssystem brechen.

Entgegen allen Bestrebungen staatlicher Sicherheitsbehörden sind wir der Meinung, daß vertrauliche Telekommunikation zwischen Menschen möglich sein muß. Abhörmöglichkeiten zur Verbrechensbekämpfung werden langfristig nicht die Verbrecher schädigen, sondern alle Menschen. In digitalen Netzen kann man Verschlüsselung zwar verbieten, verhindern kann man sie aber nicht.[17]

5 Schlußbemerkungen

Die vorangegangenen Bemerkungen zur Schlüsselerzeugung sollten zeigen, daß Interessenskonflikte durchaus tragfähige, mehrseitig sichere und akzeptable Lösungen hervorbringen können.

Trotzdem existieren für manche Probleme bisher leider keine angemessenen Lösungen. So bleibt die Frage nach einem sicheren Endgerät nach wie vor offen.

Auch dürften Entscheidungen zu einer definierten sicheren Schnittstelle zwischen Endgerät und gespeichertem Dokument notwendig sein, um zu verhindern, daß einem Nutzer ein beliebiges Dokument zur Signatur untergeschoben werden kann, während er ein anderes signieren wollte.

Der Schnittstelle zwischen Nutzer und Gesamtsystem kommt darüber hinaus die besondere Bedeutung zu, ein Umfeld zu bieten, das dem gelernten Prozeß der eigenhändigen Unterschriftsgabe nicht nachsteht. Die Echtheits- und Identifikationsfunktion der eigenhändigen

---

[17] Steganographie, d.h. Verdecken von Nachrichten, kann ein Verbrecher trotzdem anwenden. (vgl. [MöPS_94])

Unterschrift wird für digitale Signaturen als Unterschriftssurrogat unproblematisch realisierbar sein. Eine funktionierende Warnfunktion und Abschlußfunktion ist technisch schwerer zu realisieren. Allerdings wäre der Anspruch auch recht hoch, sozial gelernte Phänomene wie z.B. das „Verstehen“ der evtl. rechtsverändernden Wirkung einer Unterschrift unter ein Papierdokument auf eine nicht gegenständliche Folge von Bits zu übertragen. Im Laufe der Zeit wird aber dieses „Verstehen“ entstehen.

Um den breiten Zugang zu rechtssicherer Telekooperation zu ermöglichen, muß natürlich der Beweiswert von digitalen Signaturen geklärt sein (siehe z.B. [Bize_94]). Wir warnen davor, übereilte politische Entscheidungen zu einer vollen Rechtsgültigkeit der digitalen Signatur in allen Bereichen des Lebens zu fällen. Zunächst müssen die technischen, organisatorischen und sozialen Aspekte von digitalen Signaturen genauer untersucht und bestehende Sicherheitszweifel ausgeräumt werden.

Wir danken der Deutschen Forschungsgemeinschaft (DFG) und der Gottlieb-Daimler - und Karl-Benz Stiftung Ladenburg für die finanzielle Unterstützung. Für Anregungen, Diskussionen und Kritik geht unser Dank an Michaela Huhn, Dagmar Schönfeld und Sibylle Federrath.

6 Literatur

Ande_94 Ross J. Anderson: Why Cryptosystems Fail; Communications of the ACM 37/11 (1994) 32-40.

Aven_90 Hermann Avenarius: Kleines Rechtswörterbuch; Sonderdruck des Herder-Taschenbuches Band 1733, Bundeszentrale für politische Bildung, Bonn, 1990.

BBCM_94 Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjølsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallée, Michael Waidner: The ESPRIT Project CAFE — High Security Digital Payment Systems; ESORICS 94 (Third European Symposium on Research in Computer Security), Brighton, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

BiHa_93 Johann Bizer, Volker Hammer: Elektronisch signierte Dokumente als Beweismittel; Datenschutz und Datensicherung DuD 17/11 (1993) 619-628.

Bize_92 Johann Bizer: Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation; Datenschutz und Datensicherung DuD 16/4 (1992) 169-176.

Bize_94 Johann Bizer: Rechtliche Probleme der elektronischen Signatur; H. Kubicek, G. Müller, E. Raubold, A. Roßnagel: Jahrbuch Telekommunikation und Gesellschaft, Verlag C. F. Müller, Heidelberg 1994, Band 2: Schwerpunkt Technikgestaltung, 157-164.

BMI_95 Bundesministerium des Innern: Sicherheit im elektronischen Rechtsverkehr; hier: gesetzlicher Regelungsbedarf; Geschäftszeichen IS 6 - 606 000-3. 1/2.2, Brief vom 7. Februar 1995.

DaPP_94 Ivan B. Damgård, Torben P. Pedersen, Birgit Pfitzmann: On the Existence of Statistically Hiding Bit Commitment Schemes and Fail-Stop Signatures; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 250-265.

HaBi_93 Volker Hammer, Johann Bizer: Beweiswert elektronisch signierter Dokumente; Datenschutz und Datensicherung DuD 17/12 (1993) 689-699.

Hamm_95 Volker Hammer: Digitale Signaturen mit integrierter Zertifikatskette – Gewinne für den Urheberschafts- und Autorisierungsnachweis; Proc. Verläßliche Informationssysteme (VIS'95), Vieweg 1995, 265-274.

HePe_93 Eugène van Heyst, Torben P. Pedersen: How to make efficient Fail-stop signatures; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, 366-377.

MöPS_94 Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist; Datenschutz und Datensicherung DuD 18/6 (1994) 318-326.

PePf_95 Torben P. Pedersen, Birgit Pfitzmann: Fail-Stop Signatures; angenommen bei SIAM Journal on Computing, überarbeitete Version, 21.3.1995.

PfWa_91 Birgit Pfitzmann, Michael Waidner: Fail-stop Signatures and their Application; Securicom 91; 9th Worldwide Congress on Computer and Communications Security and Protection, Paris, 19.-22. March 1991, 145-160.

PfWa_90 Birgit Pfitzmann, Michael Waidner: Formal Aspects of Fail-stop Signatures; Interner Bericht 22/90 der Fakultät für Informatik, Universität Karlsruhe, Dezember 1990.

PPSW_95 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule; Proc. Verläßliche Informationssysteme (VIS'95), Vieweg 1995, 329-350.