Geographische Authentifikation und Signatur

Thomas Strang

German Aerospace Center (DLR)
Institut für Kommunikation und Navigation
D-82230 Wessling/Oberpfaffenhofen, Germany
thomas.strang@dlr.de

Universität Innsbruck (UIBK)
Digital Enterprise Research Institute
A-6020 Innsbruck, Austria
thomas.strang@uibk.ac.at

Abstract: Sicherheit ist ein wichtiges Thema in vielen Belangen der Nutzung mobiler Dienste. Dabei erwächst gerade aus der Mobilität neben neuen Angriffspunkten auch eine wichtige, personalisierte, ständig aktualisierte Information, die in vielerlei Hinsicht gewinnbringend verwendet werden kann: Der geographische Aufenthaltsort des Anwenders. In diesem Beitrag wird das neue Verfahren der *Geographischen Authentifikation* vorgestellt, bei dem durch geeignete Verwendung von Ortsinformationen die Sicherheit von Authentifikationsalgorithmen und Signaturverfahren verbessert werden kann.

1 Einleitung

Die wachsende Mobilität unserer Gesellschaft hat in zunehmendem Maße zur Verbreitung mobiler Endgeräte wie SmartPhones und PDAs geführt, die als Plattform in die verschiedenen Arten der Kommunikationsnetze eingebunden sind. Einerseits ergibt sich hierdurch die Notwendigkeit, bewährte Technologien im Bereich Sicherheit auf die jeweilige Netzumgebung und die darauf basierenden Anwendungen anzupassen. Einschränkungen der mobilen Geräte (z.B. CPU, Speicher und Betriebsenergie), der Funkverbindung (z.B. Bandbreite und Reichweite) und die spezifischen Angriffe in Funknetzen (Abhörangriffe, Spoofing, Impersonation, Replay, usw.) benötigen besondere Konzepte und Lösungen zur Unterstützung für die Mobilität [CK03]. Andererseits ergeben sich gerade aus der Mobilität neue Möglichkeiten. Die Möbilität der Nutzer und damit einhergehend die Mobilität der Geräte ist beispielsweise inhärente Ursache ständiger Veränderungen im Kommunikationsnetz, die Grundlage aller Untersuchungen im Forschungsgebiet der *Location Based Services* sind. In diesem Beitrag wird gezeigt, wie die Mobilität von Anwendern und Geräten in Kommunikationsnetzen ausgenutzt werden kann, um die Sicherheit von Authentifikationsverfahren zu verbessern.

Authentifikationsverfahren sind ein wichtiger Bestandteil in modernen Kommunikationsnetzen. Sie dienen der Identitätsüberprüfung, d.h. ob eine Entität (Person, Gerät, etc.) in einem System auch die Identität hat, die sie vorgibt zu haben. Gemäß [Sch96] soll die Authentifikation in Nachrichtenübertragungssystemen „dem Empfänger einer Nachricht ermöglichen, die Herkunft einer Nachricht zu ermitteln; ein Eindringling sollte sich nicht als andere Person ausgeben können“.

Häufigster Verwendungszweck von Authentifikationsverfahren ist die Identitätsprüfung eines Benutzers als Zugangs- und Rechtekontrolle für ein System. Sie können aber auch als Identitätsprüfung in der umgekehrten Richtung („verhandle ich gerade wirklich mit meiner Bank?“) bzw. in beiden Richtungen verwendet werden. Ein überwiegender Teil der in diesem Beitrag enthaltenen Beschreibungen beschränken sich exemplarisch auf den ersten Fall; die umgekehrte Richtung gilt analog. Alle Protokolle werden in dieser Thematik wie allgemein üblich bestimmten Akteuren - insbesondere „*Alice*“ (=Benutzer) und „*Bob*“ (=Host) - zugeordnet.

2 Einordnung des Verfahrens

Eine Entität (z.B. Benutzer, *Alice*) kann sich gegenüber einer anderen Entität durch Wissen (z.B. Paßwort, Geheimzahl/PIN,...), Besitz (Personalausweis, Magnetkarte, Chipkarte,...) oder Eigenschaften (Fingerabdruck, Unterschrift,...) jeweils einzeln oder in Kombination authentifizieren. Bei Authentifikation durch Wissen gilt eine Entität als glaubwürdig authentifiziert, wenn sie nachweisen kann, daß sie Kenntnis einer Information (z.B. ein Paßwort) hat, die nicht allgemein zugänglich ist. Die verifizierende Stelle (z.B. Host, *Bob*) hat ebenfalls Kenntnis von dieser Information und kann nach Übermittlung der Information überprüfen, ob die Informationen identisch sind.

Um die Vertraulichkeitsanforderungen an die das Wissen verifizierende Stelle zu erhöhen wird i.A. eine Variante der Authentifikation mit Einwegfunktionen verwendet. Diese basiert auf der Idee, daß ein Host zur Überprüfung der Zugangsberechtigung zu einem System die Paßwörter nicht kennen braucht, der Host muß lediglich gültige Paßwörter von ungültigen unterscheiden können. Dies kann durch die Verwendung von Einwegfunktionen (Hashfunktionen, z.B. MD5 oder SHA) erreicht werden, die sich in eine Richtung relativ leicht berechnen lassen, ihre Umkehrung ist aber erheblich schwieriger. Statt einer Liste von Paßwörtern speichert der Host das Ergebnis der Einwegfunktion (Hashwert $h = H(m)$) und kennt somit die eigentlichen Paßwörter nicht, so daß keine Gefahr besteht, wenn die Paßwortliste bei einem Einbruch in den Host gestohlen wird.

Da aus den von *Alice* übermittelten Daten aufgrund der Charakteristik von Einwegfunktionen nicht auf die nur *Alice* bekannte geheime Information zurückgeschlossen werden kann, schützt diese Vorgehensweise in gewissem Maß auch vor Ausspionieren der geheimen Information bei unsicheren Kommunikationskanälen (Angriffe durch Lauscher, *Eve*). Sie schützt aber nicht vor der späteren nochmaligen Verwendung („playback attack“) des abgehörten Hashwerts h durch *Eve*. Eine Lösung für dieses Problem ist die Verknüpfung des Hashwerts mit einem Zeitstempel. Die meisten der bekannten Verfahren hierzu setzen eine vertrauenswürdige dritte Instanz (*Trent*) voraus, die einen zuverlässigen Zeitstempeldienst betreibt. So kann z.B. der von Surety [Sur] in jeder Sonntagsausgabe der New York Times veröffentlichte Zeitstempel in Verbindung mit dem Diskreten Logarithmusproblem (bei $y = a^x mod p$ ist die Berechnung von y leicht, wenn a,x und p gegeben sind; die Berechnung von x gilt jedoch als nachweisbar schwer lösbares Problem, auch wenn y,a und p gegeben sind) verwendet werden, um Playback-Angriffe von *Eve* zu erschweren: *Alice* und *Bob* können immer den Zeitstempel t vom letzten Sonntag und den Hashwert

h des Paßworts unabhängig voneinander zur Berechnung von $y = t^h mod p$ verwenden. *Alice* kann das von ihr berechnete Ergebnis anschließend an *Bob* übertragen, der das Ergebnis von *Alice* mit seinen eigenen Berechnungen vergleicht. *Eve* kann jedoch selbst bei Abhören von y und Kenntnis von t und p weder h ermitteln, noch einen Playback-Angriff fahren, sobald ein neuer Zeitstempel veröffentlicht wird. Offensichtlich gewinnt dieses Verfahren an Sicherheit, wenn die Zeitstempel mit einer höheren Frequenz als einmal pro Woche generiert werden.

Dieses Problem wird systematisch mit geeigneten Challenge-and-Response Protokollen adressiert. Bei diesen wird zu Beginn jeder Kommunikationssitzung ein neuer Schlüssel generiert, mit dem die geheime Information verschlüsselt wird. Ein in der Praxis häufig verwendetes Protokoll dieser Kategorie ist CHAP [Sim96], welches jedoch einen großen Nachteil hat, wenn, wie in [Sim96] formuliert, *Bob* die geheime Information von *Alice* im Klartext kennen muß. Bessere Protokolle dieser Kategorie sind beispielsweise in [Sch96] zu finden.

3 Authentifikation über den geographischen Ort

Das Wissen, dessen Kenntnis eine Entität bei Authentifikation durch Wissen nachweist, kann vor der Verwendung durch die beteiligten Parteien (*Alice*, *Bob*, ggf. noch andere) im Prinzip frei gewählt werden. Es gibt zwar einige Regeln, die diese Wahlfreiheit einschränken, so z.B. die Verwendung von möglichst kryptischen Paßwörtern mit Sonderzeichen u.ä., um Wörterbuchangriffe und andere heuristische Angriffe zu erschweren. Auch sorgt die Verwendung von Zeitstempeln oder Challenge-and-Response Protokollen dafür, dass zu unterschiedlichen Zeiten auch unterschiedliche Daten von *Alice* an *Bob* geschickt und dort zur Verifikation herangezogen werden können. Die geheime Information an sich unterliegt jedoch keiner so hohen Dynamik. Einmal ausspioniert, z.B. durch „über die Schulter schauen“ bei der Eingabe eines Passworts, und keine Hashfunktion und kein Challenge-and-Response Protokoll schützt mehr vor Missbrauch.

Daher ist es wünschenswert, wenn das von *Alice* nachzuweisende Wissen selbst einer ständigen Änderung unterworfen ist, so dass *Alice* jedesmal aufs neue herausgefordert ist, das sich ändernde Wissen nachzuweisen. Als sich ständig änderndes Wissen bietet sich bei Authentifikationsverfahren insbesondere der aktuelle geographische Aufenthaltsort des Nutzers (*Alice*) an. Der aktuelle Aufenthaltsort unterliegt einer nutzerabhängigen Dynamik. Der aktuelle Aufenthaltsort ist dem Nutzer in der Regel bekannt oder kann über ein Positionierungsverfahren (Galileo/GPS[GLzH$^+$05], Mobilfunk, Indoor, Inertialsystem etc.) vom Benutzer ermittelt werden.

Zur Verifikation der geographischen Ortsinformation benötigt *Bob* den Zugriff auf eine Location Registry, in welcher der tatsächliche Aufenthaltsort der zu verifizierenden Entität hinterlegt ist. In Abbildung 1 ist am Beispiel einer auf dem Mobilfunksystem GSM basierenden Variante des hier vorgestellten Verfahrens gezeigt, wie *Alice* die Cell-ID der Zelle, in der ihr Endgerät gerade eingebucht ist, als Teil des persönlichen Wissens verwenden kann, um diese Information, vorzugsweise verschlüsselt, an die Bank (*Bob*) zu senden. Dieser kann über das zuständige, bereits etablierte Authentication Center (AUC)

beim Home Location Register (HLR) des Mobilfunknetzbetreibers von *Alice* nachfragen, in welcher Zelle sich *Alice* gerade aufhalten sollte.

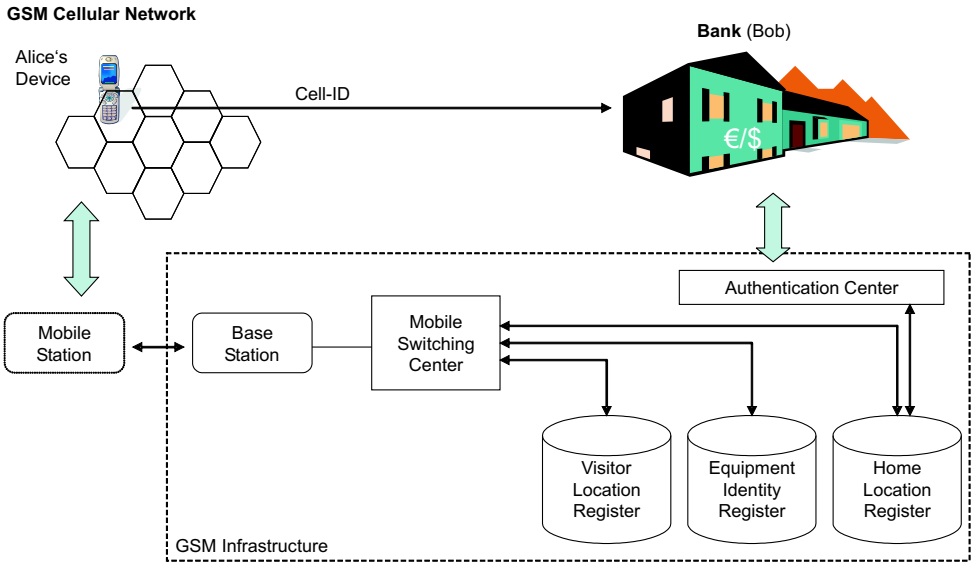

Abbildung 1: Nutzung der Positionsinformation am Beispiel von GSM

Wenn die übrigen Merkmale des jeweils verwendeten Algorithmus (z.B. Challenge-and-Response/Zeitstempel, Hashing etc.) beibehalten werden, stellt die zusätzliche Verifikation des aktuellen geographischen Aufenthaltsortes eine Erhöhung der Sicherheit des Authentifikationsverfahrens dar, da *Alice* jedesmal aufs Neue herausgefordert ist, das sich ändernde Wissen über Ihren eigenen Aufenthaltsort nachzuweisen.

Authentifikationsverfahren dieser Art könnte man sinnvollerweise unter dem Oberbegriff *Location-based Authentication (LBA)* subsummieren. Es ist bei LBA-Verfahren nicht zwingend erforderlich, dass *Bob* zur Verifikation der geographischen Ortsinformation auf Daten eines oder mehrerer Register zurückgreift, bei denen die Position von Entitäten im System hinterlegt ist. Zum einen kann *Bob* bei periodischen Verifikationen anhand einer Verteilungsfunktion über Positionsangaben [KB05] die Plausibilität der Bewegung von *Alice* überprüfen („mit Wahrscheinlichkeit p hat sich *Alice* um weniger als d Meter seit der letzten Verifikation bewegt“ oder „wie weit kann sich *Alice* in n Minuten seit dem Notruf entfernt haben“). Zum anderen wird erkannt, wenn sich *Alice* innerhalb eines gewissen Zeitfensters von zwei oder mehr unterschiedlichen Orten versucht, gegenüber *Bob* zu authentifizieren, was auch nicht plausibel ist.

Das Verfahren kann zur geographischen Authentifikation über Eigenschaften erweitert werden. Hierzu werden z.B. die Pseudorange[1]-Messungen eines Galileo/GPS-Empfängers

[1]Die Positionsermittlung erfolgt bei Satellitennavigationssystemen über die Messung der Signallaufzeiten von mehreren Satelliten zu einem Empfänger. Die Entfernungen (Ranges) sind also tatsächlich Signallaufzeiten, weshalb diese als Pseudoranges bezeichnet werden.

an eine schlüsselabhängige Hashfunktion geleitet. Der Empfänger berechnet mit dem Hashwert des Paßworts den Hashwert der Pseudorange-Werte, was als *geographischer Fingerabdruck* der aktuellen geographischen Position des Galileo/GPS-Empfängers bezeichnet wird [DM96]. Dieser geographische Fingerabdruck kann nur von *Alice* mit einem Galileo/GPS-Empfänger am aktuellen Aufenthaltsort erzeugt werden. *Bob* kann den geographischen Fingerabdruck verifizieren, indem er die Ortsinformation von einer Location Registry abfragt und mit der aktuellen Satelliten-Konstellation für die Region in Bezug bringt.

4 Ablauf des Protokolls

In Abbildung 2 wird ein exemplarischer Ablauf einer geographischen Authentifikation über Wissen dargestellt, bei der sich *Alice* gegenüber *Bob* authentifiziert. Das Beispiel ist CLARA (Challenge-by-Location and Response Authentication), eine neue Challenge-and-Response Protokollvariante, die auf dem Diskreten Logarithmus Problem basiert. Wie eingangs erläutert wird bei dieser Art von Verfahren über einen potentiell unsicheren öffentlichen Kanal zunächst ein gemeinsamer Sitzungsschlüssel K ausgehandelt, der aber selbst weder über den Kanal übertragen noch aufgrund der Charakteristik der Einwegfunktionen aus den übertragenen Daten ermittelt werden kann. Im Beispiel steht der Sitzungsschlüssel K zum Zeitpunkt t_1 sowohl *Alice* als auch *Bob* zur Verfügung.

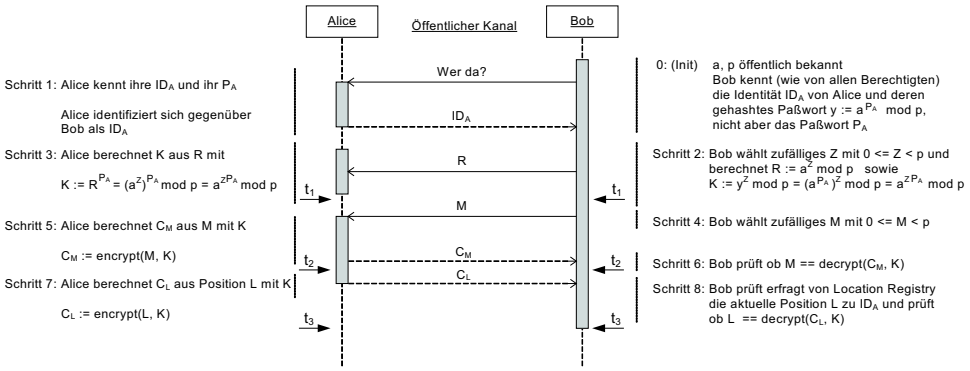

Abbildung 2: Ablauf einer geographischen Authentifikation per CLARA Protokoll

Die Schritte 4 bis 6 stellen die Verifikation per Challenge-and-Response dar, d.h. *Alice* weist die Kenntnis der geheimen Information P_A nach, ohne die sie den Sitzungsschlüssel K nicht hätte ermitteln können. `encrypt(M,K)` bezeichnet dabei eine geeignete Ver- und `decrypt(C,K)` die zugehörige Entschlüsselungsfunktion eines Datums M mit Schlüssel K. Die Schritte 0 bis 6 stellen somit im wesentlichen die übliche Vorgehensweise bei dieser Art von Authentifikationsmechanismus dar. Neu hingegen ist die Verwendung des Sitzungsschlüssels K ab Zeitpunkt t_2 zur verschlüsselten Übermittlung

(C_L) des momentanen Aufenthaltsorts L von *Alice* (z.B. die am Mobiltelefon in Abbildung 1 verfügbare Cell-ID) an *Bob* zur Verifikation mit Informationen, die *Bob* von einer Location Registry in Schritt 8 erhalten hat.

Die Schritte 7 und 8 sind zusätzlich durchzuführen und können nicht die Schritte 5 und 6 ersetzen, da die in Schritt 7 von *Alice* zu verschlüsselnden Daten C_L im Gegensatz zu M für *Alice* vorhersehbar sind, was das Authentifikationsverfahren insgesamt angreifbar macht, wenn die Schritte 5 und 6 wegfallen.

Nach diesem Verfahren steht erst zum Zeitpunkt t_3 bei Übereinstimmung der Ortsinformationen (bzw. Unterschreiten eines Schwellwertes maximaler Abweichung) die Authenzität von *Alice* für *Bob* fest (nicht aber umgekehrt).

5 Erweiterung zur geographischen Signatur

Signaturverfahren sind enge Verwandte der Authentifikationsverfahren. Die Verwandschaft ist u.a. schon darin begründet, daß die mit Signaturverfahren erzeugte elektronische Unterschrift bestimmte Eigenschaften wie Fälschungssicherheit, Einmalverwendbarkeit, Unveränderbarkeit und Unwiderrufbarkeit haben soll, zu denen auch die Authenzität der Unterschrift zählt. Dementsprechend kommen auch ähnliche Algorithmen zum Einsatz, die u.a. sicherstellen, daß der Empfänger eines Dokuments davon ausgehen kann, daß der Unterzeichner und kein Anderer ein signiertes Dokument unterschrieben hat. In Abbildung 3 ist exemplarisch das Standard-RSA-Signaturverfahren dargestellt, das auf dem Problem der Faktorisierung großer Zahlen basiert und eine Hashfunktion $H(m)$ verwendet, die nur von der Nachricht selbst abhängt.

Öffentliche Schlüssel:
n Produkt zweier (geheimer) Primzahlen p und q
e relativ prim zu $(p-1)(q-1)$

Geheimer Schlüssel:
$d := e^{-1} \; mod \; ((p-1)(q-1))$

RSA-Signatur einer Nachricht m mit dem geheimen Schlüssel d:
$s := H(m)^d \; mod \; ((p-1)(q-1))$

Verifikation der RSA-Signatur s mit dem öffentlichen Schlüssel e:
$H(M) =_? s^e \; mod \; n$

Abbildung 3: Standard RSA Signaturverfahren

Auch bei Signaturverfahren kann die Authentifizierung der zu einem Dokument gehörenden Unterschrift - und damit die Sicherheit des gesamten Signaturverfahrens - gestärkt werden, wenn es eine dynamische Komponente innerhalb des Verfahrens gibt.

Ein weiterer Nachteil üblicher elektronischer Signaturverfahren ist die Tatsache, dass die-

se bisher im Wesentlichen die Identität der die Unterschrift leistenden Instanz sowie die Zeit der Unterzeichnung eines Dokuments berücksichtigen. Informationen über den geographischen Ort der Unterzeichnung werden jedoch typischerweise nicht berücksichtigt. Tatsächlich ist aber die Information über den Ort der Unterschriftsleistung ein wichtiger Bestandteil von Verträgen und Beurkundungen. So fordert z.B. die geltende Rechtsprechung in den meisten Ländern, dass bestimmte Dokumente nur dann rechtskräftig sind, wenn neben der Unterschrift des Unterzeichners auch der Ort der Unterzeichnung angegeben wird. Siehe hierzu folgendes Beispiel, welches ein Auszug aus *BGB §2247 (Eigenhändiges Testament)* darstellt:

> (2) Der Erblasser soll in der Erklärung angeben, zu welcher Zeit (Tag, Monat und Jahr) und an welchem Ort er sie niedergeschrieben hat.
>
> (5) Enthält ein ... Testament keine Angabe über die Zeit der Errichtung und ergeben sich hieraus Zweifel über seine Gültigkeit, so ist das Testament nur dann als Gültig anzusehen, wenn sich die notwendigen Feststellungen über die Zeit der Errichtung anderweitig treffen lassen. Dasselbe gilt entsprechend für ein Testament, das keine Angabe über den Ort der Errichtung enthält.

Bei Signaturverfahren kann die Authenzität der Unterschrift auf ähnliche Weise wie bei Authentifikationsverfahren durch die Berücksichtigung einer Ortsinformation im Unterschrifts- und Verifikationsalgorithmus gestärkt werden. Gleichzeitig wird hierdurch den gesetzlichen Forderungen nach Informationen über den Ort der Unterschriftsleistung als wichtiger Bestandteil von Verträgen und Beurkundungen nachgekommen. Wo und an welcher Stelle die Ortsinformation in den jeweiligen Algorithmus einfließt, hängt vom jeweiligen Algorithmus und von der gewünschten Aussagekraft ab.

Die Ortsinformation kann z.B. vor der Unterschriftsleistung mit dem Dokument konkateniert werden, wodurch beide Infomationen zu einer Einheit verschmelzen, da durch die nachfolgende Signatur die Unveränderlichkeit und damit auch die Untrennbarkeit gewährleistet werden.

> Geheimer/Öffentliche Schlüssel wie beim Standard RSA Signaturverfahren.
>
> Erweiterte RSA-Signatur einer Nachricht m mit geheimem Schlüssel d:
> $s := H(m, \mathbf{location})^d \ mod \ ((p-1)(q-1))$
>
> Verifikation der erweiterten RSA-Signatur s mit öffentlichem Schlüssel e:
> $H(M, \mathbf{location}) =_? s^e \ mod \ n$

Abbildung 4: Geografisches RSA Signaturverfahren

Die Ortsinformation kann aber besser noch als Eingabe-Schlüssel für eine schlüsselabhängige Hashfunktion $H(m, k)$ verwendet werden. Die meisten der gängigen Signatur- und zugehöriger Verifikationsverfahren wie RSA (siehe Abbildung 3) oder DSS/DSA [Sch96] setzen gewöhnlich sowohl bei der Signaturfunktion als auch bei der dazu passenden Verifikationsfunktion bereits schlüsselunabhängige Hashfunktionen ein. Wenn bei diesen

Verfahren die schlüsselunabhängigen Hashfunktionen $H(m)$ durch schlüsselabhängige Hashfunktionen $H(m,k)$ ersetzt und Informationen über den Ort der Unterzeichnung als Eingabe-Schlüssel für diese schlüsselabhängigen Hashfunktionen verwendet werden (siehe Abbildung 4), sind die zuvor geschilderten positiven Effekte zu erzielen, ohne gleichzeitig das zu unterzeichnende Dokument an sich verändern zu müssen.

Analog hierzu kann beim Digital Signature Algorithm (DSA, siehe Abbildung 5), der Bestandteil des Digital Signature Standard (DSS) ist, vorgegangen werden.

Öffentliche Schlüssel:
p Primzahl der Länge $x * 64$ mit $x \geq 8$
q 160 Bit langer Primfaktor von $(p-1)$
g := $h^{(p-1)/q} \; mod \; p$, wobei h eine beliebige Zahl $\leq p-1$ ist, so daß $g > 1$ ist
y := $g^x \; mod \; p$

Geheimer Schlüssel:
x := beliebige Zahl $x < q$

DSA-Signatur (r,s) einer Nachricht m mit geheimem Schlüssel x und Zufallszahl $k < q$:
r := $(g^k \; mod \; p) \; mod \; q$
s := $(k^{-1}(H(m) + xr)) \; mod \; q$

Verifikation der DSA-Signatur (r,s):
w := $s^{-1} \; mod \; q$
$r =_? ((g^{(H(m)*w) \; mod \; q} * y^{(rw) \; mod \; q}) \; mod \; p) \; mod \; q$

Abbildung 5: Standard DSA Signaturverfahren

Auch hier kann die schlüsselunabhängige Hashfunktion $H(m)$ durch eine schlüsselabhängige Hashfunktionen $H(m,k)$ ersetzt und Informationen über den Ort der Unterzeichnung als Eingabe-Schlüssel für diese schlüsselabhängigen Hashfunktionen verwendet werden (siehe Abbildung 6).

Geheimer/Öffentliche Schlüssel wie beim Standard RSA Signaturverfahren.

Erweiterte DSA-Signatur (r,s) einer Nachricht m mit geheimem Schlüssel x und Zufallszahl $k < q$:
r := $(g^k \; mod \; p) \; mod \; q$
s := $(k^{-1}(H(m, \mathbf{location}) + xr)) \; mod \; q$

Verifikation der erweiterten DSA-Signatur (r,s):
w := $s^{-1} \; mod \; q$
$r =_? ((g^{(H(m,\mathbf{location})*w) \; mod \; q} * y^{(rw) \; mod \; q}) \; mod \; p) \; mod \; q$

Abbildung 6: Geografisches DSA Signaturverfahren

6 Zusammenfassung und Ausblick

In diesem Beitrag wurde gezeigt, wie durch die Integration von Informationen über den aktuellen geographischen Aufenthaltsort des Anwenders eines mobilen Endgeräts die Gewißheit über die Korrektheit der Identität des Anwenders für einen Interaktionspartner gestärkt werden kann. Hierzu wurde exemplarisch anhand des neuen Protokolls CLARA gezeigt, wie bekannte Authentifikationsprotokolle erweitert werden können, um eine zusätzliche Verifikation einer Identität über Ihren aktuellen Aufenthaltsort bzw. einer maximal tolerierten Abweichung von einer vorgegebenen oder angenommenen Position zu ermöglichen. In einem nächsten Schritt wird die praktische Nutzbarkeit des neuen Verfahrens, d.h. der geografischen Authentifikation, anhand einer Referenzimplementierung für mobile Endgeräte wie Mobiltelefone validiert werden. Durch die Verwandheit von Authentifikationsalgorithmen mit Signaturverfahren können ähnliche Ansätze ebenfalls gewinnbringend bei Signaturverfahren eingesetzt werden, womit neben dem Sicherheitsgewinn gleichzeitig gesetzlichen Forderungen nach Informationen über den Ort der Unterschriftsleistung genüge getan wird. Interessant für zukünftige Untersuchungen ist insbesondere die Frage, in welcher Form die Ortsinformationen vorliegen müssen, um einerseits hinreichend genau den Aufenthaltsort des Anwenders zu spezifizieren und andererseits hinreichend weich zu sein, um dem Grundrecht auf Privatsphäre nachzukommen.

Literatur

[CK03] Sumith Chandratilleke und Michael Kreutzer. Credential-basierte Ad-hoc-Authentifikation. *netzwoche Netzguide E-Security 2003*, Marz 2003.

[DM96] Dorothy E. Denning und Peter F. MacDoran. Location-Based Authentication: Grounding Cyberspace for Better Security. *Computer Fraud and Security*, Februar 1996.

[GLzH+05] Adam Giszczak, Barbara Lenz, Michael Meyer zu Hoerste, Thoralf Noack, Hans-Peter Schäfer, Marius Schlingelhof, Thomas Strang und Detlef Zukunft. GALILEO im Verkehr. Bericht, DLR, Mai 2005.

[KB05] Frank Kargl und Alexander Bernauer. The COMPASS Location System. In *International Workshop on Location- and Context-Awareness (LoCA 2005), Oberpfaffenhofen, Germany, May 12-13, 2005*, Jgg. 3479 of *Lecture Notes in Computer Science*, Seiten 105–112. Springer, 2005.

[LS92] B. Lloyd und W. Simpson. RFC 1334: PPP Authentication Protocols, Oktober 1992. Obsoleted by RFC1994 [Sim96]. Status: PROPOSED STANDARD.

[Sch96] Bruce Schneier. *Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C*. Addison-Wesley, Bonn, Germany, 1996.

[Sim96] W. Simpson. RFC 1994: PPP Challenge Handshake Authentication Protocol (CHAP), August 1996. Obsoletes RFC1334 [LS92]. Status: DRAFT STANDARD.

[Sur] Surety. The Surety Digital Notary Service.