

## **4. XML Signaturworkshop**

14.-15. April 2005

XML-Uni, BSI und GI Fachgruppe ECOM

TU Ilmenau, Hotel Tanne, 98693 Ilmenau

### ***Stichwortprotokoll***

*R. Grimm, 15.4.2005 / update tt.mm.2005*

#### **Teilnehmer:**

Grimm (TU Ilmenau), Steiert (Teletrust), Horstmann (bos), Rümpler (TUI Studentin Wirtschaftsinformatik), Lautsch (XML-Uni), Farnbacher (izn), Psarros (Uni Bochum), Schmidt (BSI), Schadow (Salt-Solutions), Herrmann (Software AG), Kessler (Software SAG), Weber (Software AG), Thommes (TUI Student der MT), Prauß (BSI), Riedle (XML-Uni), Beyer (TUI wiss. Mitarbeiterin)

#### **Begrüßung durch R. Grimm (XML-Uni, TU Ilmenau), A. Schmidt (BSI)**

#### **Signaturpraxis (Moderation Grimm)**

##### **1. A. Schmidt, BSI Bonn: Präsentation einer sicheren Signaturerstellungseinheit als Client Tool der Virtuellen Poststelle (VPS)**

Architektur der VPS. OSCI = Online Service Computer Interface zum Transport abgesicherter Daten auf Anwendungsebene, mit Sicherungsumschlägen. VPS auf der Basis von OSCI organisiert.

Vor allem Behandlung der Client-Komponente. Intuitiv, einfach, am „Look-and-feel“ von Outlook orientiert. Wird eingesetzt bei Bundessozialgericht und Bundesfinanzhof. Geschlossene Benutzergruppe incl. Anwälte und Staatsanwaltschaft, auch miteinander kompatibel.

VPS und Trusted Computing. Sichere Signaturerstellungseinheiten. TrustList zugelassener Prozesse, dezentral oder zentral angeboten.

Von Nutzern als wichtig angesehen und akzeptiert: Authentizität von Nachrichten, Transparenz des Signaturvorgangs, sichere Umgebung (TrustList), dass es keine 100%ige Sicherheit gibt, wird akzeptiert. Spätere Entwicklung: Bürgerservices, z.B. Elster, Bafög, Rente usw.

Wie viel Last darf man den Bürgern zum Aufbau einer sicheren Clientkomponente zumuten? Festlegung von vertrauenswürdigen Prozessen in der TrustList?

##### **2. D. Schadow, Salt-Solutions München: Eclipse XML-Security Plug-In; Präsentation eines Signaturtools**

Zielgruppe: Anwender mit XML-Grundkenntnissen zum Erlernen der Funktionsweise von XML Verschlüsselung und Signatur. Vorbild CrypTool.

Ausführungsplattform ist Eclipse, XML-API von Apache. Funktionskomponenten des Plug-In: Kanonisierung, Signieren/Verifizieren, Verschlüsselung. Eine Online-Hilfe enthält theoretische Erläuterungen zu Grundlagen der XML-Sicherheit, sowie zur Verwendung des Plug-Ins. Einstellungsassistent, Signaturassistent, Verschlüsselungsassistent, Entschlüsselungsassistent.

Praktische Vorführungen. Ausblick auf weitere Entwicklung. Farbliche Hervorhebung selektierter Dokumentteile. XML-Spy (noch nicht). Externer Crypto-Provider.

## **Praxis der Standardisierung I (Moderation Grimm)**

### **3. Marc Horstmann, bremen online services: XKMS in der Praxis: Anwendung des Protokolls**

XML Key Management Spezifikation. 1. X-KRSS: Registrierung, Widerruf, Wiedergewinnung (Recovery), ist bei bos nicht implementiert. 2. X-KISS: Anfrage, Bezug und Verifikation öffentlicher Schlüssel. XKMS definiert keine PKI, keine Trust-Policy, fokussiert auf XML-Signature und XML-Encryption. XKMS: die Prüfung von XML-Signature KeyInfo durch einen externen Server unterstützen.

Locate-Service: Auffinden von Zertifikaten aufgrund von KeyInfo-Element oder <UseKeyWith>. <KeyUsage> in verschiedenen Kontexten, z.B. S/MIME oder PKIX.

ValidateRequest. Auskunft über Status eines Zertifikats.

XKMS erfüllt die VPS-Anforderungen nur zum Teil. Ok: Zertifikate lokalisieren, prüfen; teilw. ok: Zertifikate bereitstellen (registrieren); schwierig: verschiedene Formate. Der XKMS-Service in VPS ist das OCSP/CRL-Relay. ValidateRequest und CompoundRequest sind implementiert, Key Registration (noch?) nicht. Signierte Anfragen sind möglich. Probleme mit OpaqueClientData (Senden beliebiger Daten von Client an Server). Certificate Extensions.

ToDo's, vor allem „Was muss XKMS Service können, um ISIS-MTT kompatibel zu sein?“

### **4. Peter Steiert, Teletrust Erfurt: European Bridge-CA: Gesamtarchitektur und Zielsetzung**

Ziel: Verknüpfung von PKI-Inseln. Voraussetzung: gemeinsames Sicherheitsverständnis, gemeinsame Dienste;  $n^2$ -Problem. Lösung: Bridge-CA als „Single Point of Administration“. Einsatz von X.509-Zertifikaten.

Lösung: Einfacher Zugriff („just click and go“). Zentraler Bridge-Verzeichnisdienst, vor allem für Verschlüsselungszertifikate. Explizite Anfragen (keine Wildcard-Abfragen).

Validierungsdienst („just click and verify“), als Mittler, nicht in der rechtlichen Verantwortung. Bridge-CA signiert ihre Antworten.

Vorteile: Medienbruchfreie sichere Kommunikation über PKI-Unternehmensgrenzen hinaus. Skalierbarkeit, dadurch Investitionsschutz für Unternehmen. Bridge CA als zentraler Vertragspartner, internationale Standards, Stammzertifikatsaustausch, Verzeichnisdienst, Überprüfungsdienst, Vorgabe einer Mindestpolicy anstatt Policy-Mapping. Die Einzelpolicies sind für die Teilnehmer untereinander einsehbar, aber nicht öffentlich.

Kooperation zwischen vielen verschiedenen Partnern, Board-Mitglieder von Teletrust, Deutsche Bank, Siemens, DaimlerChrysler, Allianz, BSI, Telekom u.a.

## **Elektronische Archivierung (Moderation Schmidt)**

### **5. Wolfgang Farnbacher, izn Hannover: Elektronische Langzeitarchivierung in der Praxis – Vorstellung verschiedener Ansätze**

Traditionell: Papier/Haltbarkeit, Text-Inhalt, Unterschrift, Siegel/Originalität, ohne Hilfsmittel unmittelbar lesbar. Digital/elektronisch: Bitmuster, Absicherung und Lesbarkeit nur mit technischen Mitteln. Frage: Gerichtsverwertbarkeit?

Projekt ArchiSig mit Fraunhofer SIT (Pordesch), Datev, Uni Kassel (Roßnagel), Ergebnis in Buchform erhältlich.

Technische Archivierung. Strategie: 5-7 Jahre, Daten unveränderlich. Elektronische Dokumente unterliegen zeitlich rasch veränderlichen technischen Verarbeitungsmethoden. Gründe: Formatevielfalt, Änderung der Formate, mangelnde Standardisierung, Daten in Datenbanken sind ohne DBMS wertlos,

Lösungsansätze: Festlegung von Formaten, vor Signatur Transformation in ein Aufbewahrungsformat (z.B. TIF), Annahmeregeln für fremde Dokumente, Datenbankinformationen sind in Dokumente zu überführen. Achtung bei Transformation in Aufbewahrungsformat vor (!) Signatur: das greift in den Kommunikationsprozess der Dokumentenerstellung ein; aber XML-Quelltext wäre u.U. auch ein akzeptables Aufbewahrungsformat.

Elektronische Signaturen sind heute nicht auf Langzeitsicherung ausgelegt. Probleme: Signaturtypen, Signaturstandards, zusätzliche Verifikationsdaten, Signaturalterung. Lösungsansätze: Vermeiden überflüssiger Signaturen, Anpassung Stufe an Dauer, Verifikationsdaten ausreichend vollständig, Signaturneuerung mit qualifiziertem Zeitstempel, Hashwertbäume nach ArchiSig-Konzept.

Sonderproblem Transformation. Formatttransformationen zerstören digitale Signaturen.

Beispiel Niedersachsen: 200 Mio Seiten Papier jährlich zu den Akten (Altregistratur), 10 Mio Seiten Papier ins 10-Jahresarchiv, davon 1% signiert: 100 Tausend Seiten signiertes Papier jährlich ins 10-Jahresarchiv.

Architekturmodell elektronischer Archivierung. Langzeitformate sind XML-Container mit Metadaten und über die zu archivierenden Dokumente und Dokumenteninhalte als Payload.

Projektschwerpunkte Dokumentenerstellung, Dokumentenmanagement und Verfahrensintegration, Langzeitspeicher und elektronisches Staatsarchiv, dabei auch angedacht: Online-Zugriff mit Rollen und Rechten. Stand April 2005: Konzept weitgehend abgeschlossen, Langzeitspeicher und el. Staatsarchiv in Testbetrieb; Dokumentannahme und -abgabe durch Virtuelle Poststelle in Planung, Konzepte zur Dokumenttransformation (aus anderen Projekten) in Planung.

### **6. Thomas Prauß, BSI Bonn: Juristische Anforderungen an die elektronische (Langzeit-)Archivierung**

Bisher keine einheitliche Regelung zur elektronischen Archivierung. Einzelne Fachgesetze. Wechselwirkung zwischen Erstellung und Archivierung, Einfluss von Datenschutz und Geheimhaltung.

„Wie“ der Archivierung: Grad der Identität, Ort der Aufbewahrung, Verfügbarkeit und Zugang. Beispiele der Aufbewahrungspflichten: z.B. qualifizierte Zertifikate 5 bzw. 30 Jahre, Buchführungsunterlagen 6 bzw. 10 Jahre, Personalakten der Beamten 5 Jahre nach Abschluss, Akten von Rechtsanwälten und Steuerberatern 7 Jahre, Ärztliche Aufzeichnungen 10 Jahre (Satzungsrecht), dosimetrische Messdaten von AKW-Mitarbeitern mindestens 30 Jahre (die Frist kann sich durchaus auch leicht verdoppeln).

Besondere Regelungen für den elektronischen Gerichtsverkehr, Justizkommunikationsgesetz, Aufbewahrungsfristen 6 Monate bis 120 Jahre. Dauernde Aufbewahrung der Register und insbesondere des Grundbuchs!

Neben Aufbewahrungspflichten gibt es Aufbewahrungsinteresse: Dies ist potentiell unbegrenzt! Beweisbedarf zur Abwehr von Ansprüchen und zur Begründung eigener Ansprüche, dabei Verjährungsfristen 3 bis 30 Jahre.

Besondere Regelungen potentiell in allen Rechtsgebieten!

Archivierung von Verifikationsdaten und sonstigen Hilfsdaten. Für elektronische Rechnungen Dokumentation der Ergebnisse der Signaturprüfung, bei qualifizierten Signaturen zusätzliche Verifikationsdaten. Anforderung nach Signaturneuerung und Formatkonvertierungen (bisher aufwändig über Beglaubigungen).

Wichtige Rahmenbedingungen des Daten- und Geheimnisschutzes. Dazu Sicherung der Vertraulichkeit, Skalierung von Zugriffsrechten. Sperrung, Berichtigung oder Löschung einzelner Daten innerhalb von Dokumenten kann erforderlich sein, das hat Einfluss auf die Signatur.

## **Praxis der Standardisierung II (Moderation Schmidt)**

### **7. Marc Horstmann, bremen online services: Technische Szenarien für gesetzeskonforme Massensignaturen**

Siehe auch FAQ Nr. 18 der RegTP. Individualsignaturen: ein bewusster Signaturakt (PIN) pro Dokument. Batchsignaturen: Mengen gleichartiger Dokumente in einem Akt signiert, zum Beispiel Rechnungen der gleichen Art. Einschränkungen von Zeitraum oder Anzahl für die Freigabe der Identifikationsdaten von RegTP gefordert.

VPS geht aber darüber hinaus, da die Inhalte, die durch die VPS gehen, unterschiedlichster Art sind und das Signieren in Anzahl oder Zeitraum nicht beschränkt ist. Dafür etwa der Modul NetSigner. Anwendungsbeispiel OSCI-Manager mit inhaltlich gleichartigen Antworten: Zeitliche Beschränkung?

Diskussion der Signaturstufe: Wieso sind hierfür qualifizierte Signaturen erforderlich? Würden Zeitstempelsignaturen ausreichen? Inhaltliche Prüfung? Entscheidend ist die Aussagekraft der Signatur: Willenserklärung versus Wissenserklärung.

Szenario 1a der ein für alle Mal frei geschalteten Karte auf dem Signaturserver. Anderes Szenario 1b der individuell an den NetSigner mitgelieferten verschlüsselten PIN, die dieser entschlüsselt, verifiziert und zur Kartenfreigabe nutzt (z.B. für Bestellvorgänge). Weiteres Szenario 3a starke Signatur. Weiteres Szenario 3b PIN/TAN. Was davon wäre RegTP-konform? BSI auch erst in der Diskussion.

Achtung genau zu unterscheiden zwischen technischen Szenarien und Anwendungsszenarien. Wissenserklärungen sind von Willenserklärungen zu unterscheiden.

## **8. E.G. Giessmann, T-Systems Nova: Aktuelle Standardisierungsaktivitäten bei ETSI**

--- ausgefallen ---

### **Zusammenfassung und Ausblick**

Anwendungen auf dem Weg: Virtuelle Poststelle.

Transparenz der Signaturverfahren durch Ausbildung gut vorangekommen: Signaturtool.

Hilfsfunktionen der Infrastruktur auf dem Wege: XKMS, Bridge-CA.

Neue Anwendungsprobleme Archivierung, Massensignaturen.

Einfluss von Datenschutz auf Signaturen und ihre Anwendungen (Archivierung).

Neue Sicherheitsaufgaben in den aufkommenden Web-Services: neues Thema insbesondere für XML-Signaturen.

Standardisierung im Fluss, ebenfalls weiter zu beobachten.