Certification Practice Statement

Version 1.0, Stand: 2015/12/03 09:40

Dieses Dokument beschreibt den Betrieb der „Certification Authority“ des datenkollektiv.net. Es handelt sich um eine Version, die noch geändert und ergänzt werden kann, so lange die Grundsätze dieses Dokumentes nicht verletzt werden.

Zweck des CPS

Mit diesem Dokument möchten wir nach außen nachvollziehbar machen

- warum wir eine CA betreiben
- auf welche Prozeduren wir uns geeinigt haben, um sicher zu arbeiten
- für wen wir unter welchen Umständen Zertifikate ausstellen

Um das CPS nachvollziehen zu können ist eine Idee davon, wie und wozu Zertifikate genutzt werden hilfreich.

Warum arbeiten wir mit einem eigenen Rootzertifikat?

Die Verschlüsselungsinfrastruktur des Netzes beruht auf Vertrauen - Regionalisierung bietet eine Chance für gerechtfertigtes Vertrauen. Im regionalen Umfeld sind viele Mittel (z.B. Flyer mit Fingerprint) möglich, um die Echtheit der Zertifikate zu prüfen.

Wie stellen wir Zertifikate aus?

Um sicherzugehen, dass

a) unsere Zertifikate ein gewisses Maß an Sicherheit bieten und
b) niemand ausser uns Zertifikate in unserem Namen ausstellt

haben wir uns auf bestimmte Verfahrensweisen geeinigt, die wir im Folgenden für Euch und uns dokumentieren.

Offline CA

Unsere CA wird auf extra dafür eingerichteten und nur zu diesem Zweck genutzten Systemen ohne Zugang zum Netzwerk betrieben.

Algorithmen

Unser Stammzertifikat hat eine Schlüssellänge von 4096 bit. Als Signaturalgorithmus verwenden wir SHA-256 + RSA.

Laufzeiten

Das Stammzertifikat hat eine Laufzeit von 32 Jahren, die Zwischenzertifikate von 4 Jahren.

4-Augen-Prinzip

Die privaten Schlüssel für unsere CA's sind verschlüsselt und verteilt abgelegt. Nur wenn wenigstens zwei von uns zusammenkommen kann eine Zertifikatsanfrage unterschrieben werden. Jede/r besitzt ein anderes Stück des privaten Schlüssels. Dieser wird vor dem Gebrauch zusammengesetzt und danach wieder gelöscht. Es kann also keine/r allein im Namen des Datenkollektivs Zertifikate generieren.

Selbstbeschränkung der Möglichkeiten

Wo möglich schränken wir die von uns generierten Zertifkate ein, um Mißbrauch zu erschweren. Da geschieht zum Beipiel, indem wir die möglichen Verwendungsarten (z.B. als Serverzertifikat) oder auch die Anzahl der möglichen Zwischeninstanzen beschränken.

Backup

Für den Fall der Fälle existiert ein Backup unserer PKI bei einem Treuhänder, das nur unter klar definierten Bedingungen herausgegeben wird und nur bei Kenntnis des geheimen Schlüssel-Passwortes von Nutzen ist.

Für wen stellen wir Zertifikate aus?

Primärer Zweck unserer CA ist es, unsere eigenen Dienste abzusichern. Wir halten uns jedoch die Möglichkeit offen, auch für andere Menschen oder Institutionen Zertifikate zu generieren. Zertifikate werden nur bei persönlichem Kontakt ausgestellt und wenn sichergestellt werden kann, dass die Person/Institution über die Domain verfügt.