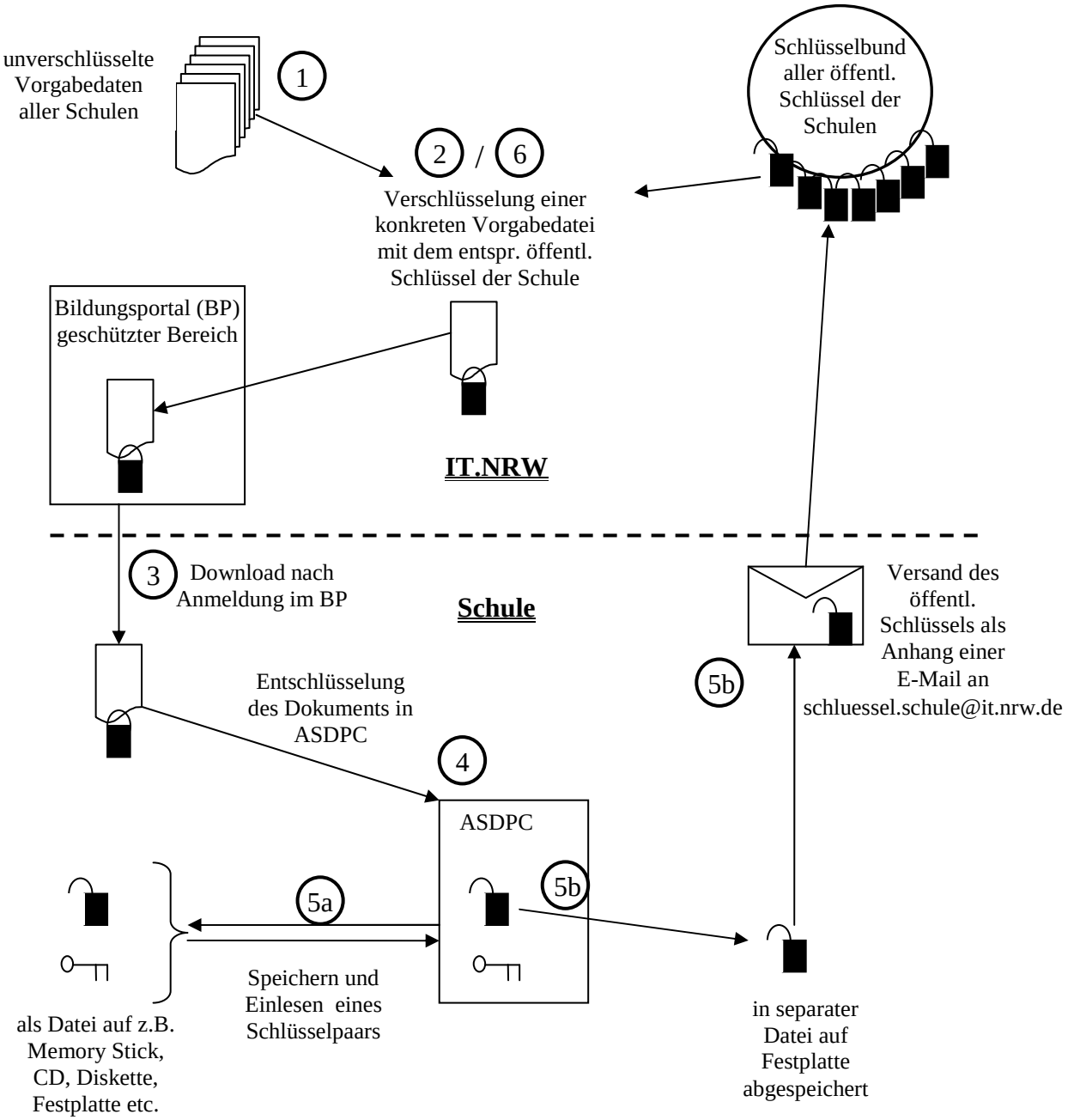
Informationen zum Verschlüsselungsverfahren



Legende:

…20080626_102953.pub Datei = öffentlicher Schlüssel (Vorhängeschloss)

…20080626_102953.sec Datei = privater Schlüssel

20080626 = Erstellungsdatum: 26.06.2008

102953 = Erstellungsuhrzeit: 10:29:53 (Std:Min:Sek)

Generelles zum Verfahren der asymmetrischen Verschlüsselung

Die sichere Kommunikation zwischen IT.NRW und den Schulen basiert auf einem sog. Public Key bzw. asymmetrischen Verschlüsselungsverfahren. Der öffentliche Schlüssel stellt bildlich gesprochen eine Art Vorhängeschloss dar, mit welchem IT.NRW z. B. Ihre Vorgabedaten (oder SchIPS-Daten,…) nach außen hin unlesbar machen kann. Nur Sie als alleiniger Besitzer des passenden privaten Schlüssels können dieses „Vorhängeschloss“ wieder öffnen. Um die Handhabung der Schlüssel zu unterstützen, schreiben wir in jeden Dateinamen einer verschlüsselten Datei neben der Schulnummer das Erstellungsdatum und die Erstellungsuhrzeit der Schlüssel (siehe Bild auf der ersten Seite).

Anhand des Schaubilds auf der ersten Seite geben wir Ihnen umfassende Hintergrundinformationen zum gesamten Prozess der Verschlüsselung, der es uns erstens erlaubt, Dateien sicher von IT.NRW zu den Schulen zu transferieren und zweitens in der umgekehrten Richtung Erhebungsdaten sicher von den Schulen nach IT.NRW zu verschicken. Die hier beschriebenen Punkte (3) bis (5a+b), die bei den Schulen angesiedelt sind, werden in der Vorgehensanleitung auf der beiliegenden CD konkret mit Bezug zu den jeweiligen relevanten Menüpunkten in ASDPC erläutert.

Teil 1 – Sicherer Dateitransfer IT.NRW ⟹ Schule

(1) **Schützenswerte Dateien für die Schulen (IT.NRW):** IT.NRW hält Daten (Dateien) für Sie bereit, die besonders schützenswert sind, weil sie z.B. personenbezogene Daten beinhalten (z.B. Lehrerdaten innerhalb der Vorgabedaten, SchIPS-Daten,…).

(2) **Verschlüsselung (Kryptifizierung) der Dateien (IT.NRW)**: Sie haben uns in der Vergangenheit mindestens einmal ihren öffentlichen Schlüssel geschickt, den wir seitdem verwenden, um die für Ihre Schule bestimmte Datei zu verschlüsseln (bildlich entspricht dies dem Schließen des Vorhängeschlosses). Nur Sie als Inhaber des einzigen passenden privaten Schlüssels können diese Verschlüsselung wieder aufheben.

(3) **Ihr persönlicher Download (Schule)**: Diese Datei können Sie dann im geschützten Bereich des Bildungsportals herunterladen. Jetzt wäre auch ein guter Zeitpunkt, sich die ASD-Signatur (siehe Teil 2) zu notieren.

(4) **Einlesen/Entschlüsseln der Datei (Schule)**: Sowohl im Bildungsportal als auch in ASDPC werden Sie über Generierungsdatum und –uhrzeit des öffentlichen und privaten Schlüssels Ihrer Schule informiert. Nur wenn diese Angaben übereinstimmen, kann nun das Einlesen und Entschlüsseln der Vorgabedaten mittels ASDPC bzw. SchILD-NRW funktionieren.

(5) **Wenn die Schlüssel nicht übereinstimmen (Schule)**: Sollten Sie in ASDPC keinen passenden privaten Schlüssel haben, so können Sie zwei Wege gehen:

(5a) **Import und Export von Schlüsselpaaren (Schule)**: ASDPC und SchILD-NRW bieten Möglichkeiten zum Import und Export der von Ihnen mittels ASDPC selbst generierten Schlüsselpaare. So können Sie das passende Schlüsselpaar, falls es in der Vergangenheit abgespeichert wurde, nun wieder einlesen.

(5b) **Generieren eines neuen Schlüsselpaares (Schule)**: Sie können mit ASDPC jederzeit und beliebig oft ein neues Schlüsselpaar generieren. Der öffentliche Schlüssel wird als Datei abgespeichert, so dass Sie diesen Schlüssel IT.NRW bekannt machen, indem Sie ihn als Anhang einer E-Mail an folgendes Postfach von IT.NRW senden: schluessel.schule@it.nrw.de.

(6) **Neue Verschlüsselung mit neuem Schlüssel (IT.NRW)**: IT.NRW nimmt den von Ihnen gesendeten neuen öffentlichen Schlüssel entgegen. Dieser ersetzt am „großen Schlüsselbund“ Ihren alten Schlüssel. Innerhalb kurzer Zeit wird automatisiert für Ihre schützenswerten Dateien im Bildungsportal eine neue Verschlüsselung, wie unter Punkt (2) beschrieben, durchgeführt, so dass Sie Ihre neu verschlüsselten Dateien abholen können (Punkt (3)).

Teil 2 – Sicherer Dateitransfer Schule ⟹ IT.NRW

Hintergrund:

Um Ihre Erhebungsdaten verschlüsselt an IT.NRW senden können, verwenden wir das gleiche Verfahren wie oben in Teil 1 beschrieben mit vertauschten Rollen. Da in diesem Fall allerdings nur ein einziger Empfänger, nämlich IT.NRW, existiert, ist das Vorgehen erheblich einfacher. Genau wie Sie, hat IT.NRW ein einziges Schlüsselpaar generiert und den einen öffentlichen Schlüssel (offenes Vorhängeschloss) fest in ASDPC integriert. Jede Schule, die nun Erhebungsdaten erstellt, verschlüsselt die Daten mit dem gleichen Schlüssel von IT.NRW. Nur IT.NRW selber besitzt den passenden privaten Schlüssel und kann anschließend die Datei wieder entschlüsseln.

ASD-Signatur:

Beim Erstellen der Erhebungsdaten kommt allerdings ein weiterer Punkt hinzu. ASDPC fragt Sie beim Erstellen der Erhebungsdaten nach der ASD-Signatur Ihrer Schule. Diese ASD-Signatur erfahren Sie ebenfalls im geschützten Bereich des Bildungsportals nach erfolgreicher Anmeldung. Dazu melden Sie sich bitte auf der Seite http://www.schulministerium.nrw.de/BP/SVW mit Kennwort und Passwort an. Ihre ASD-Signatur können Sie z.B. hier notieren:

Ihre ASD-Signatur:	