

Interview mit Christian Weber für Amazee

Claudia Roy:

Herr Weber, in den Medien und auch hier in der Community wird immer wieder die Sicherheit der SuisseID bezweifelt. Wie sicher ist die SuisseID wirklich?

Christian Weber:

Die SuisseID wurde gemeinsam mit den vier Anbietern Post/SwissSign, Swisscom, QuoVadis und BIT gemäss den strengen Auflagen des Bundesgesetzes über die elektronische Signatur (ZertES) und unter Berücksichtigung von internationalen Sicherheitsstandards spezifiziert und entwickelt.

Auf was für einem Prinzip basiert die SuisseID?

Die SuisseID basiert auf dem Prinzip der Public Key Infrastructure und verwendet zertifizierte Kryptochips (Smartcards), eine Kombination von Technologien, deren Sicherheit weltweit anerkannt und seit Jahren bewährt ist. Auch andere Staaten geben elektronische Identitäten nach dem Muster der SuisseID heraus (Beispiel: Bürgerkarte in Österreich usw.).

Kann meine Identität gestohlen werden?

Will ein Angreifer die elektronische Identität oder digitale Signatur eines anderen missbräuchlich verwenden, stehen ihm sehr hohe Hürden entgegen. Er muss die SuisseID (Karte/Stick) physisch besitzen oder online Zugriff haben und das Passwort kennen. Denn zum einen muss die SuisseID Karte (resp. USB-Stick) im Computer eingesetzt sein, zum anderen ist die Kenntnis des geheimen Passwortes nötig, um die SuisseID überhaupt zu aktivieren.

Am besten ist dieser Prozess mit der Bankkarte vergleichbar, wo ein Bargeldbezug nur möglich ist, wenn beide Sicherheitselemente vorliegen, Bankkarte plus PIN. Darum dürfen SuisseID Inhaber niemals das Passwort und die Karte zusammen aufbewahren. Die SuisseID Nummer, ein Element aus dem Zertifikat, und das Passwort in elektronischer Form allein können nicht missbräuchlich verwendet werden. Im Gegensatz dazu reicht bei einer Kreditkarte der Besitz der Karte, um mit den aufgedruckten Daten (Kartenummer, Name & Vorname, Enddatum und dreistellige Nummer) im Internet einzukaufen.

Was hat die SuisseID für eine Sicherheitsaufgabe?

Es ist wichtig, die SuisseID in ihrer Eigenschaft als Sicherheitselement für die elektronische Identität und digitale Signatur von anderen Sicherheitsaufgaben abzugrenzen. Sicherheit bezieht sich immer auf bestimmte Aspekte. Die SuisseID ist sicher bezüglich Identitätsnachweis und elektronischer Signatur. Selbstverständlich gibt es Anwendungen, bei denen andere Aspekte hinzukommen, wie z.B. wenn eine hohe Sicherheit des Übertragungskanals gewährleistet werden muss. Zu denken ist da etwa an E-Banking oder der Zugriff auf nachrichtendienstliche Anwendungen. In solchen Fällen kann man ebenfalls die SuisseID einsetzen, der Übertragungskanal jedoch muss dann aber mit weiteren Sicherheitselementen ergänzt werden.

Die SuisseID ist ein hervorragendes Sicherheitselement, wenn es in einer sicheren Umgebung eingesetzt wird. Es liegt in der Verantwortung jedes einzelnen Anwenders, sein PC vor Schadprogrammen zu schützen und sich entsprechend vorsichtig im Internet zu bewegen.

Wird die SuisselD überarbeitet?

Nach der nochmaligen Überprüfung des Sicherheitskonzeptes der SuisselD mit Experten sehen wir keinen Anlass im Konzept etwas zu ändern. Da die Sicherheit und damit das Vertrauen in die SuisselD eminent wichtig sind, setzen wir die laufenden Sicherheitsuntersuchungen mit internen (BIT) und externen Experten (Fachhochschulen und spezialisierte Unternehmen) fort. Periodische Anpassungen nach dem neusten Stand der Technologie werden wenn nötig vorgenommen.

Das heisst konkret:

Die SuisselD ist so sicher wie ein extern an einen PC angeschlossener Chip sein kann. Gehen wir von den folgenden zwei möglichen Szenarien aus, welche einer SuisselD passieren könnten:

Szenario 1: Jemand findet eine SuisselD-Karte oder einen Stick auf der Strasse. Der Finder hat also den PIN-Code dazu nicht. Die SuisselD ist nicht zu knacken und nach drei falschen Pin-Eingabeversuchen endgültig gesperrt und kann auch nicht wieder aktiviert werden.

Szenario 2: Ein PC ist mit Trojanern verseucht und ich benutze die SuisselD auf diesem Gerät. Was passiert? Wie bei allen anderen Systemen auch, ist solange die SuisselD eingesteckt ist, auch hier ein Gefahrenpotential vorhanden. Dies ist jedoch kein SuisselD-spezifisches Problem, sondern betrifft generell alle Smartcard-Lösungen.

Es gibt Möglichkeiten, einen Angriff durch Trojaner zu erschweren. Beispielsweise können spezifische Kartenleser der Klasse 2 oder 3 in Kombination mit spezifischer Middleware eingesetzt werden. Solche Komponenten sind aber nur begrenzt verfügbar und relativ teuer, da sie immer einen aufwändigen Zertifizierungsprozess durchlaufen müssen. Ein Angriff durch spezialisierte Trojaner kann so aber auch nicht Verhindert werden.

Die SuisselD erhebt nicht den Anspruch, den PC des Anwenders gegen alle möglichen Gefahren abzusichern. Sie ist lediglich ein sicheres Element für den sicheren Identitätsnachweis und die sichere Erstellung rechtsgültiger elektronischer Signaturen. Es liegt in der alleinigen Verantwortung des Anwenders, sein PC vor Schadprogrammen zu schützen und sich entsprechend im Internet zu verhalten.

Ein weiterer Punkt, welcher kritisiert wird. Ist die Usability der SuisselD. Was hat die SECO hier für eine Meinung?

Ja, die Usability kann noch verbessert werden. Bitte bedenken Sie dabei, dass die SuisselD erst seit dem 3. Mai im Verkauf ist und wir sind nach wie vor mit dem Release 1 unterwegs. Die Anbieter sind auf dem Weg dies so rasch wie möglich zu verbessern.

Was könnte an der SuisselD aus Ihrer Sicht verbessert werden?

Klar: die Usability. Daran müssen wir arbeiten.

Vielen Dank, dass Sie sich die Zeit genommen haben für dieses exklusive Interview für die Amazee Community der SuisselD.

Claudia Roy