Atos Information Technology GmbH ·
Otto-Hahn-Ring 6 · 81739 München

Peter Kiefer
Otto-Hahn-Ring 6
81739 München
T +49-211-399-22575
M +49-163-1668218
atos.net/de
Peter.Kiefer@atos.net

Please scroll down for english version

München, 19. Okt. 2017

Kundeninformation:
RSA-Schlüsselgenerierung mit CardOS V5

Sehr geehrte Damen und Herren,

hiermit möchten wir Sie über ein potentielles Sicherheitsproblem der CardOS-V5-Produkte bei der RSA-Schlüsselgenerierung informieren, das seinen Ursprung in der „Asymmetric Crypto Library (ACL)" der SLE78 Chip Plattform von Infineon hat. Ein Forscherteam der Masaryk-Universität in Tschechien hat eine Methode entwickelt, mit der eine mathematische Schwäche eines bestimmten Algorithmus zur Primzahlgenerierung identifiziert werden konnte. Die Methode erlaubt eine vereinfachte Berechnung des privaten Schlüssels eines RSA-Schlüsselpaars mit Hilfe des entsprechenden öffentlichen Schlüssels. Bei bestimmten RSA-Schlüssellängen resultiert dies in einer deutlichen Verringerung der kryptographischen Stärke.

Betroffen sind insbesondere RSA-Schlüssel mit 2048 und 4096 Bit, die auf der Karte generiert werden. Nach aktuellem Kenntnisstand reduziert sich der Aufwand zur Berechnung bei RSA-2048 im Mittel auf unter Hundert CPU-Jahre, der Aufwand bei einem 4096-Bit-Schlüssel liegt schätzungsweise bei 10^9 CPU-Jahren. RSA-Schlüssel mit 3072 und 3584 Bit Länge sind nicht betroffen, da die mathematische Schwäche des Algorithmus bei diesen Schlüssellängen nicht zum Tragen kommt.

Alle anderen kryptographischen Dienste wie Ver- und Entschlüsselung, Signaturerzeugung und -verifikation, sowie Kryptographie basierend auf Elliptischen Kurven und symmetrische Kryptographie sind nicht betroffen. Ebenso ist die Chip-Hardware (symmetrische und asymmetrische Co-Prozessoren) nicht betroffen.

Alle CardOS-V4-Produkte sind nicht von diesem Problem betroffen, da sie auf einer anderen Chip-Plattform implementiert sind.

Falls Sie die RSA-Schlüsselgenerierung auf der Karte mit CardOS-V5-Produkten nutzen, sollten Sie auf Applikationsebene eine Risikobewertung durchführen und entsprechende Maßnahmen ergreifen.

Es gibt mehrere Lösungsansätze, die vom Einsatzfeld der Karten abhängig sind:

(1) Nutzt der Kunde die Karten als Sichere Signaturerstellungseinheit (SSCD), um qualifizierte elektronische Signaturen zu erstellen, bleibt nur die Möglichkeit, RSA-3072- oder RSA-3584-Bit-Schlüssel einzusetzen, da diese Schlüssellängen nicht von dem Problem betroffen sind. Das

Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits Common Criteria Maintenance Verfahren für 'CardOS V5.0 with application for QES, V1.0' und 'CardOS V5.3 QES V1.0' durchgeführt, die die Zertifizierung auf die RSA-Schlüssellängen 3072 und 3584 Bit einschränken. Ferner wurde eine Nachtragsbestätigung für CardOS V5.0 entsprechend dem Deutschen Signaturgesetz mit derselben Einschränkung durchgeführt. Das Zentrum für sichere Informationstechnologie in Österreich (A-SIT) hat die Bescheinigung der CardOS V5.3 nach Österreichischem Signaturgesetz mit der Einschränkung der Schlüssellängen bestätigt. Für weitere Details wenden Sie sich bitte an Atos.

(2) Kunden, die nicht auf eine formale Zertifizierung angewiesen sind, haben mehrere Optionen:

(i) Nutzung der Atos Service Packages

Atos hat Service Packages für die CardOS-V5.x-Karten entwickelt, die entweder bei der Initialisierung oder auch nachträglich auf die Karten geladen werden können, sofern die entsprechenden Zugriffsrechte vorliegen. Mit diesen Service Packages wird das Problem der Crypto Library vollständig behoben (durch Nutzung einer alternativen Schlüsselgenerierungs-Funktion unter Berücksichtigung einer längeren Schlüsselgenerierungszeit). Die neue Version der CardOS-Middleware, CardOS API V5.4, beinhaltet diese Service Packages bereits in den aktuellen Initialisierungsskripten. Sofern Karten unabhängig von der CardOS API in der Produktion initialisiert werden, sind die entsprechenden Skripte um die neuen Service Packages zu erweitern. Bei Karten, die bereits im Feld sind, muss der Kunde entscheiden, ob er das Service Package nachlädt und danach das Zertifikat zurückruft, um neue Schlüssel zu generieren. Falls Sie Support für das Nachladen der Packages auf die Karten benötigen, kontaktieren Sie bitte Atos.

(ii) Externe Generierung von RSA-Schlüsseln beliebiger Länge und Import auf die Karte.

(iii) Nutzung von RSA-Schlüsseln der Länge 3072 oder 3584 Bit.

Wir möchten Sie bitten, diese Informationen auch an Partner und Kunden weiterzuleiten.

Sollten Sie weitere Fragen haben, dann wenden Sie sich gerne an uns.

Mit freundlichen Grüßen

Atos Information Technology GmbH

Munich, 19. Okt. 2017

Customer Information:
RSA Key Generation with CardOS V5

Dear ladies and gentlemen,

we would like to inform you of a potential security issue regarding all CardOS V5 products, which is related to RSA key generation based on the Infineon "Asymmetric Crypto Library (ACL)" of the SLE78 chip platform. A researcher team of the Masaryk University, Czech Republic, recently found a method to identify mathematical weaknesses of particular algorithms for prime number generation. The method allows simplified calculation of the private key of the RSA key pair with the knowledge of the respective public key. Certain RSA key lengths are considered to be significantly weakened in cryptographic strength.

In particular, RSA keys with 2048 and 4096 bit, which are generated on the card, are affected. According to current knowledge the effort for calculating RSA-2048 is reduced on average to below hundred CPU years, the effort for calculating RSA-4096 is estimated to be 10^9 CPU years. RSA-3072 and RSA-3584 keys are not affected, since the mathematical weakness of the algorithm does not apply at these key lengths.

All other RSA cryptographic services – encryption, decryption, signature generation, and verification – as well as Elliptic Curve based cryptography and symmetric cryptography are not affected. The chip hardware (symmetric and asymmetric co-processors) is also not affected.

All CardOS V4 products are not affected by this issue, since they are implemented on a different chip platform.

If you are using on-card RSA key generation with CardOS V5, a risk-assessment on application level should be performed and corresponding measures should be undertaken.

There are several options to mitigate the problem depending on the card application:

(1) If the customer uses the products as certified Secure Signature Creation Device (SSCD) to generate qualified electronic signatures, there is the option to change to RSA-3072 or RSA-3584, since both key lengths are not affected by the problem. The Federal Office for Information Technology in Germany (BSI) already performed Common Criteria Maintenance processes for both ‘CardOS V5.0 with application for QES, V1.0’ and ‘CardOS V5.3 QES V1.0’, which limit the certification to the RSA key lengths 3072 and 3584 bit. In addition there is a re-confirmation of CardOS V5.0 acc. to German Signature Law with the same RSA key lengths limitation. The Secure Information Technology Center in Austria (A-SIT) has confirmed CardOS V5.3 according to Austrian Signature Law with the same limitation of RSA key lengths. For further details please contact Atos.

(2) Customers not requiring a formal certification have several options:

(i) Usage of Atos Service Packages

Atos developed Service Packages for all CardOS V5 products, which can be loaded during the initialization process or even after card issuing, if the access rights allow this. Those Service Packages completely fix the issue of the crypto lib (by using an alternative method for key generation taking into account a longer key generation time). The new version of our middleware, CardOS API V5.4 already contains initialization scripts including those CardOS Service Packages. If cards are initialized w/o using the CardOS API in the production process the respective initialization scripts need to be updated with the new Service Packages. For cards in the field the customer has to decide, whether the Service Package shall be loaded and the certificate shall be withdrawn in order to generate new keys. For the update of cards please contact Atos for any tool support.

(ii) External generation of RSA keys with arbitrary key length and import to the card.

(iii) Usage of RSA keys with 3072 or 3584 bit key length.

Please forward this information to your customers and/or partners.

In case you have any questions please do not hesitate to get in contact with us.

With best regards

Atos Information Technology GmbH