



Ihre neue AWB Multicard



Sie haben heute Ihre neue AWB Multicard erhalten. Damit Sie sämtliche Funktionen der neuen Karte kennenlernen und einrichten können, erhalten Sie die folgenden Dokumente:

1. Erste Schritte mit der AWB Multicard
2. Anleitung AWB Multicard für Secure Printing einrichten
3. Anleitung Umschlüsseln
4. Rechte und Pflichten der Zertifikatsinhaber der Swiss Government PKI

Übrigens: alle Anleitungen und Merkblätter finden Sie auch auf unserer Webseite unter www.armee.ch/awb



1. Erste Schritte mit der AWB Multicard

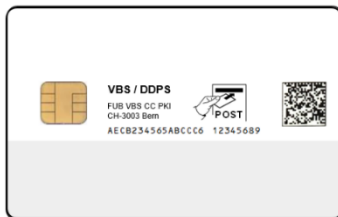
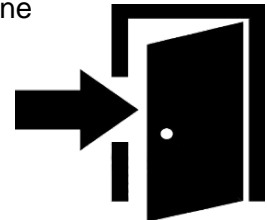


Zeitmanagement

Die Zeiterfassung wird am **Folgetag** nach Erhalt der AWB Multicard automatisch funktionieren.

Zutritte

Nach dem Ausstellen Ihrer neuen AWB Multicard haben Sie noch keine Zutrittsrechte. Die Zutritte müssen Sie bei Ihrer "Zutrittsbewilligungsinstanz" für die AWB Multicard für jeden Standort neu beantragen. Nähere Infos zu Ihrer "Zutrittsbewilligungsinstanz" finden Sie auf www.armee.ch/awb. Setzen Sie gleich den RFID-PIN für die Zutrittskontrolle (wird nur für ausgewählte Standorte wie z.B. das VZ VBS in Bern benötigt). Detaillierte Infos zum Setzen des RFID-PIN erfahren Sie im "*Leitfaden RFID PIN setzen*".

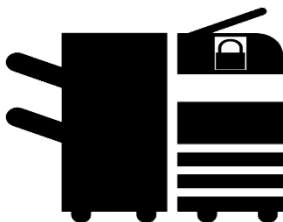
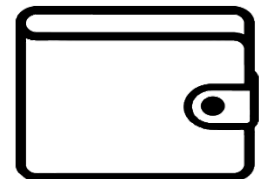


Smartcard

Auf der Rückseite der AWB Multicard befindet sich Ihre Swiss Government Smartcard. Die Prozesse der Smartcard bleiben gleich. In der Anleitung "*Umschlüsseln*" erfahren Sie Schritt für Schritt wie Sie allfällige verschlüsselte E-Mails und Dokumente entschlüsseln können.

Geldmanagement

Auf der AWB Multicard befinden sich zwei elektronische "Geldbeutel" welche an unterschiedlichen Standorten und Automaten verwendet werden. Bei einem Verlust, Defekt oder Wechsel der AWB Multicard kann Ihr Guthaben **nicht** zurückerstattet werden. Verbrauchen Sie Ihr Guthaben auf Ihrem alten Badge, bevor Sie ihn retournieren.



Secure Printing

Wird die AWB Multicard für das Secure Printing verwendet, muss diese neu registriert werden. Nähere Infos dazu erfahren Sie in der Anleitung "*Secure Printing*".

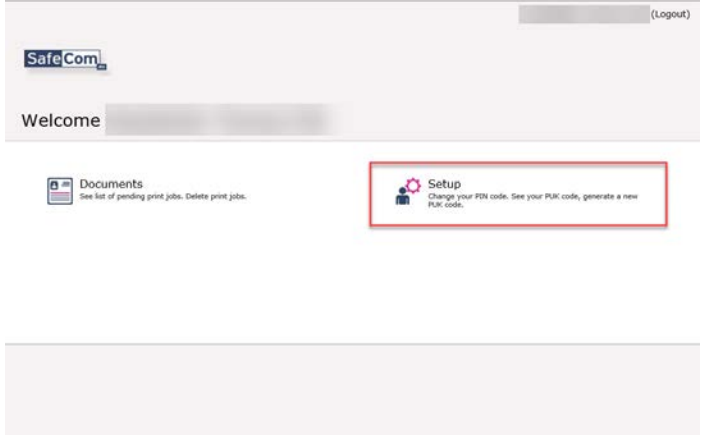
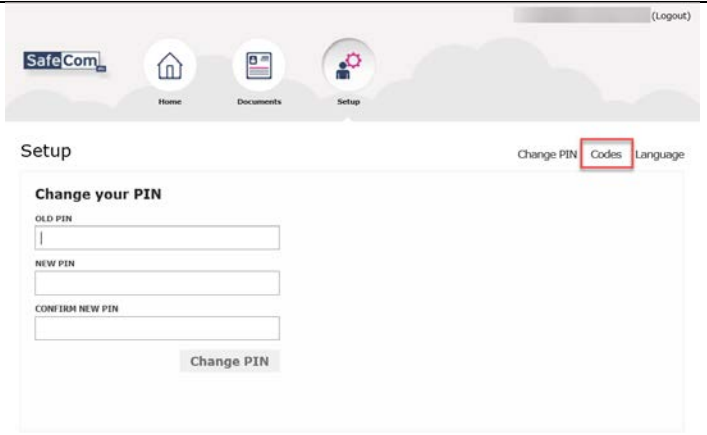
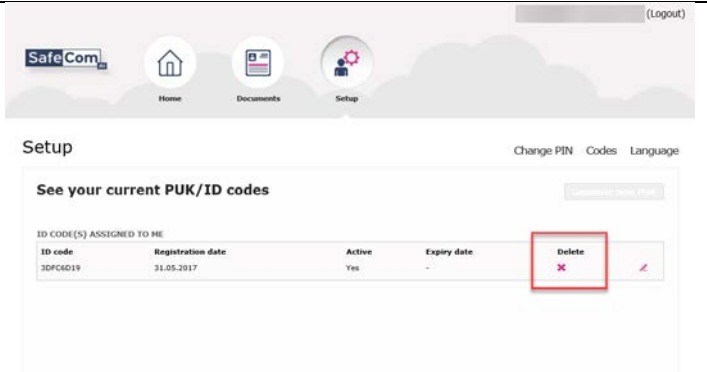
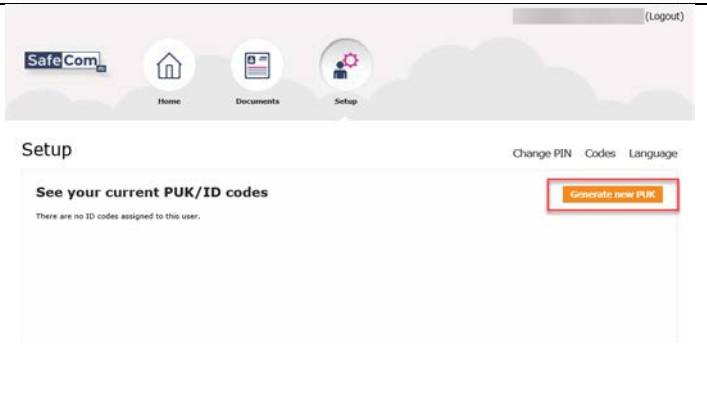
AWB Daten

Unter <https://intranet.awb.vbs.admin.ch/awb-wp-server/> können Sie Ihre eigene Badge History einsehen und bei Bedarf Ihr Foto und Ihre Unterschrift herunterladen.

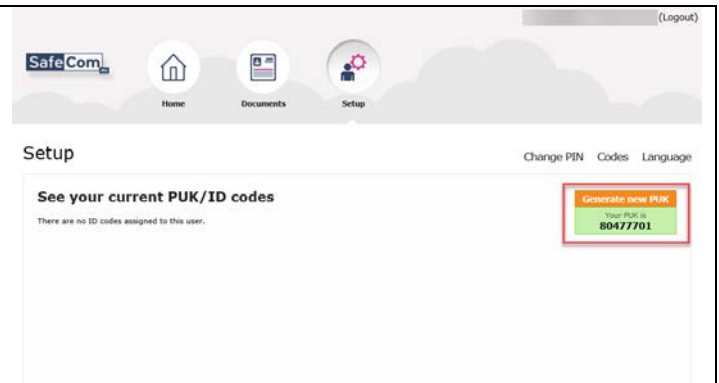




2. Anleitung AWB Multicard für Secure Printing einrichten

<p>1. Öffnen Sie an Ihrem BURAUT Arbeitsplatzsystem das SafeCom Webinterface via http://secprint.ifc1.ifr.intra2.ad-min.ch/ und drücken Sie auf Setup.</p>	
<p>2. Klicken Sie auf Codes (Deutsch: PUK-Nr.)</p>	
<p>3. Falls Sie Secure Printing bisher noch nicht genutzt haben, können Sie diesen Schritt überspringen. Wenn Sie bisher Secure Printing genutzt haben, müssen Sie nun die bisher registrierte Smart-card mittels delete löschen.</p>	
<p>4. Drücken Sie auf Generate new PUK (Deutsch: Neue PUK Nr. erstellen)</p>	

5. Ihr PUK wird nun angezeigt.
Notieren Sie sich diese Nummer.



6. **Variante HP Multifunktionsgerät**

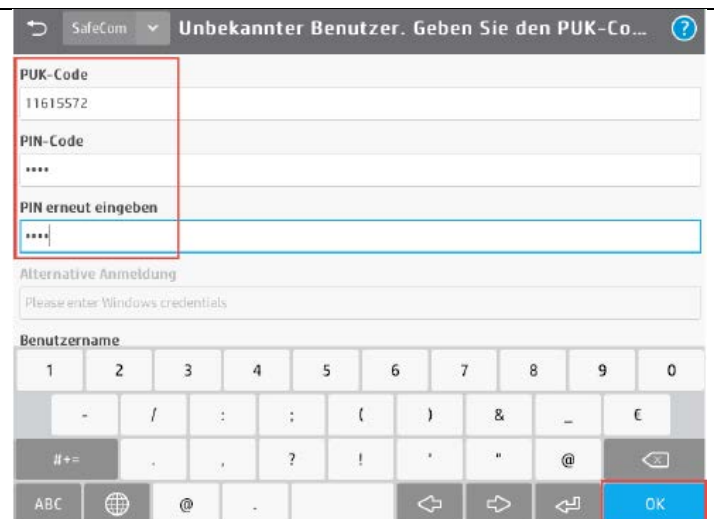
Begeben Sie sich an Ihr bevorzugtes Multifunktionsgerät und streifen Sie Ihre AWB Multicard über den integrierten Kartenleser.



Die AWB Multicard nicht auf dem Leser liegen lassen, dies kann zu Störungen führen.

7. Sie werden nun aufgefordert Ihren 8-stelligen PUK einzugeben und einen PIN Code einzugeben.

Der PIN Code ist persönlich und darf nicht weitergegeben werden. Jede Smartcard muss nur einmal registriert werden. Es spielt keine Rolle ob die Erstanmeldung an einem Xerox oder HP Gerät erfolgt. Nach einer erfolgreichen Erstanmeldung können sämtliche BURAUT Drucker mit der SafeCom Lösung uneingeschränkt benutzt werden.



8. Variante XEROX Multifunktionsgerät

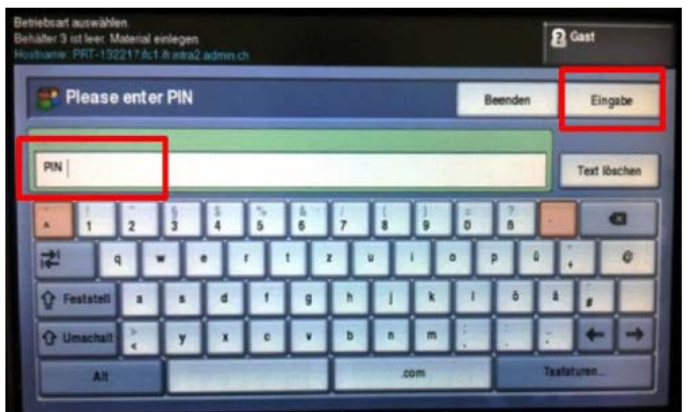
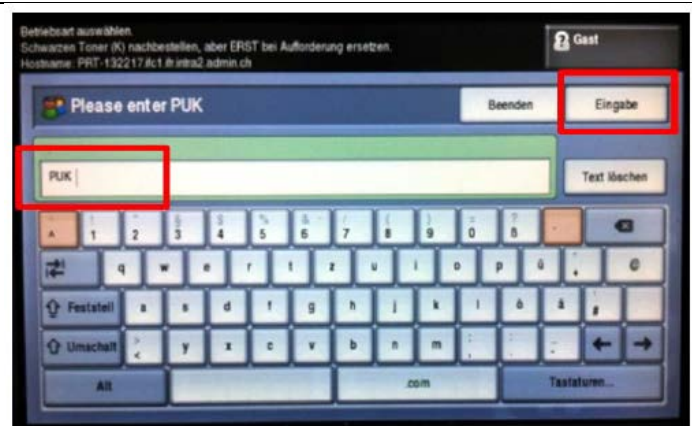
Begeben Sie sich an Ihr bevorzugtes Multifunktionsgerät und streifen Sie Ihre AWB Multicard über den integrierten Kartenleser.

Die AWB Multicard nicht auf dem Leser liegen lassen, dies kann zu Störungen führen.



9. Sie werden nun aufgefordert Ihren 8-stelligen PUK einzugeben und einen PIN Code einzugeben.

Der PIN Code ist persönlich und darf nicht weitergegeben werden. Jede Smartcard muss nur einmal registriert werden. Es spielt keine Rolle ob die Erstanmeldung an einem Xerox oder HP Gerät erfolgt. Nach einer erfolgreichen Erstanmeldung können sämtliche BURAUT Drucker mit der SafeCom Lösung uneingeschränkt benutzt werden.





3. Anleitung Umschlüsseln

Aufgrund des Smartcardwechsels müssen Ihre E-Mails und Dateien welche verschlüsselt sind umverschlüsselt werden, damit sie mit der neuen Smartcard wieder lesbar sind. Der untenstehende Prozess erklärt Ihnen die verschiedenen Schritte, welche zu erledigen sind.

Erledigen Sie die Prozesse frühestens 24h nach dem Wechsel der AWB Multicard, jedoch innerhalb einer Woche.

1.



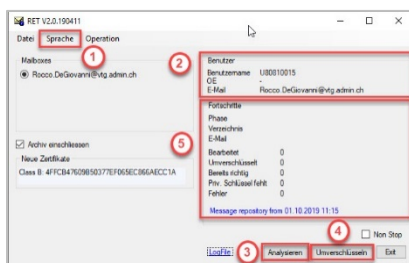
Sie haben bereits eine Registrierstelle aufgesucht und haben vor Ort eine neue AWB Multicard bezogen.

2. Umschlüsselung der E-Mails im Outlook



Stecken Sie Ihre **neue** AWB Multicard in den Kartenleser und melden Sie sich auf Ihrem PC an. Stecken Sie danach zusätzlich Ihre **alte** Smartcard in einen externen Kartenleser (erhältlich bei Ihrem Superuser). Warten Sie mind. 30 Sek. und starten Sie dann das Outlook-Umschlüsselungs-Tool.

Start - Alle Programme - Swiss Government PKI - Outlook RET



- ① Hier kann die Sprache geändert werden.
- ② Hier wird Ihre Account-Nummer und Ihre E-Mailadresse angezeigt.
- ③ Damit die Umverschlüsselung aktiv wird müssen Sie zuerst auf Analysieren klicken und abwarten bis dieses sämtliche Mails gefunden hat.
- ④ Klicken Sie auf "Umverschlüsseln". Das gesamte Postfach wird nun umgeschlüsselt.
- ⑤ Hier wird die Statistik angezeigt.
Hinweise: Sie werden teilweise nach dem PIN Ihrer Smartcard gefragt, geben Sie diesen ein, damit die E-Mails umgeschlüsselt werden können.



Statistik:

Bearbeitet: Null (0) bearbeitet heisst, Sie haben keine verschlüsselten E-Mails, somit ist der Vorgang ebenfalls abgeschlossen.

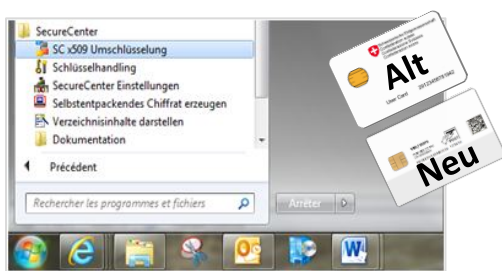
Umverschlüsselt: Sie sehen wie viele E-Mails umverschlüsselt wurden.

Fehler: Die angezeigte Anzahl E-Mails konnte, aufgrund eines Fehlers¹, nicht umgeschlüsselt werden.

Differenz: Wenn eine Differenz zwischen "Bearbeitet" und "Umverschlüsselt" besteht, besitzen Sie entweder nicht

mehr alle alten Schlüssel² oder Sie haben bereits chiffrierte E-Mails mit dem Schlüssel der neuen Smartcard erhalten.

3. Umschlüsselung der Dateien mit SecureCenter

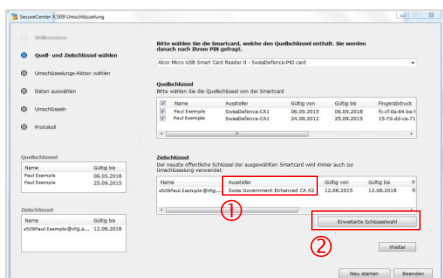


Starten Sie das SecureCenter-Umschlüsselungs-Programm und klicken Sie auf weiter.

Start – Alle Programme – SecureCenter – SC x509 Umschlüsselung

Hinweise: Sie werden nach dem PIN Ihrer Smartcard gefragt, geben Sie diesen ein, um weiterzufahren.

Falls Sie dieses Programm nicht finden, wurde es nicht installiert. Dieser Prozessschritt ist somit erledigt, gehen Sie direkt zum Pt 4.



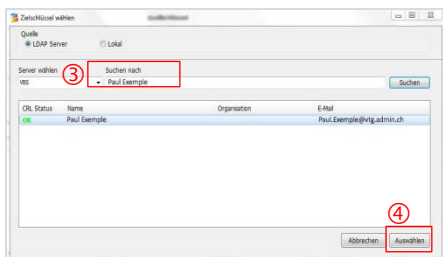
Kontrollieren Sie, dass beim Zielschlüssel unter "Aussteller" **1**, Swiss Government steht und **das Gültigkeitsdatum das Datum ist an dem Sie die neue AWB Multicard erhalten haben**. Wenn das nicht der Fall ist, müssen Sie unter "Erweiterte Schlüssel" **2**, im Suchfeld mit Ihrem Namen und Vornamen **3**, den richtigen Schlüssel suchen und auswählen **4**. Kontrollieren Sie nochmals den Zielschlüssel und klicken Sie auf weiter.

Auf der nächsten Seite wählen Sie "Automatische Wahl". Alle Ihre Dateien werden durchsucht.

Klicken Sie danach auf "Umschlüsselung starten".

Mit der Anzeige des Protokolls ist die Umschlüsselung abgeschlossen. Das Protokoll listet allfällige Fehler³ auf.

Hinweis: Die Meldung "Keine Dateien gefunden" bedeutet dass Sie keine Dateien mit SecureCenter verschlüsselt haben. Der Vorgang ist somit ebenfalls abgeschlossen.



4.



Wenn Sie die Schritte 2 und 3 erfolgreich durchgeführt haben, behalten Sie die alte Karte noch mind. einen Monat und kontrollieren Sie, ob alle E-Mails und Dateien wieder lesbar sind. Wenn in dieser Zeit keine Fehler aufgetreten sind, muss Ihre alte Karte **zwingend an das CC PKI FUB, Stauffacherstrasse 65, 3003 Bern versendet werden**. Benutzen Sie nur noch die neue AWB Multicard.

Weitere allgemeine Informationen über die Smartcard finden Sie im Internet der Schweizer Armee unter:

Service - Informationen für die Truppe - Smartcard

http://www.vtg.admin.ch/de/service/info_trp/smartcard.html

¹ Melden Sie sich beim Helpdesk FUB (058 465 22 22)

² Sie müssen ein Key Recovery auf der alten Smartcard beantragen (siehe Internet Schweizer Armee – Service – Informationen für die Truppe - Smartcard – Swiss Government PKI - Key Recovery)

³ Für weitere Informationen zu den Fehlermeldungen siehe "Kurzanleitung Umschlüsselungstools SecureCenter". (Internet Schweizer Armee – Service – Informationen für die Truppe – AWB Multicard – Kurzanleitungen - Umschlüsselungstool SecureCenter)



4. Rechte und Pflichten der Zertifikatsinhaber der Swiss Government PKI (PublicKeyInfrastructure)

Sehr geehrte/r Zertifikatsinhaber/in

Für Sie wurde eine Smartcard der Schweizerischen Eidgenossenschaft ausgestellt.

Neu:



Alt:



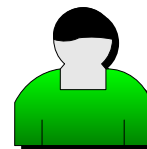
Diese Smartcard ist Ihr digitaler Ausweis, mit dem Sie Ihre Identität beim Anmelden an einen VBS Computer und bei verschiedenen Applikationen nachweisen können.

Wenn ein Benutzer Ihre Smartcard mit dem richtigen PIN-Code (**P**ersönliche **I**dentifikations-**N**ummer) freischalten kann und wenn die Smartcard weder abgelaufen noch gesperrt ist, geht die Applikation davon aus, dass es sich um Sie persönlich handelt.

Für die Applikation gilt:



nicht abgelaufen
nicht gesperrt + richtigen PIN-Code =



Paul Exemple

Alle Transaktionen werden dann unter Ihrem Namen durchgeführt und Sie können unter Umständen für diese Transaktionen zur Rechenschaft gezogen werden.

Sie sind deshalb aufgefordert, mit Ihrer Smartcard sorgfältig umzugehen und haben folgende Pflichten:

Rechte und Pflichten der Zertifikatsinhaber der Swiss Government PKI

1. Bei der Verwendung der Smartcard gelten grundsätzlich die "Weisungen über die Nutzung der Informatikmittel VBS (Informatiknutzungsweisungen VBS)".
2. Ihre Smartcard ist persönlich. Solange sie nicht gelöscht oder zerschnitten ist, dürfen Sie die Smartcard **nie** an eine andere Person weitergeben, auch nicht zu Reparaturzwecken. Ausnahmen: nach dem Löschen/Revozieren durch die Registrationsstelle (die Karte muss dem RA-Officer übergeben werden).
3. Bewahren Sie Ihre Smartcard so auf, dass sie nicht in Besitz einer anderen Person gelangen kann.
4. Wenn Sie Ihren PIN-Code wechseln beachten Sie bitte, dass Sie einen sicheren PIN-Code wählen. Ein solcher besteht aus mindestens 6 Zahlen und stammt **nicht** aus dem Geburtsdatum von Ihnen oder Ihren Angehörigen, Ihrer Telefonnummer, Ihrem Autokennzeichen oder anderen leicht zu ermittelnden Zahlenkombinationen.
5. Halten Sie Ihren PIN-Code geheim und schreiben Sie ihn unter keinen Umständen auf die Smartcard.
6. Ändern Sie den PIN-Code sofort, wenn Sie wissen oder vermuten, dass Dritte ihn kennen. Falls nicht ausgeschlossen werden kann, dass diese auch Zugriff zur Smartcard hatten, müssen Sie eine RA informieren (Telefonnummer der HauptRA: siehe unten).
7. Wenn Sie bemerken, dass Ihnen die Smartcard abhandengekommen ist, melden Sie sich unverzüglich bei einer RA (Telefonnummer der HauptRA: siehe unten) und lassen Sie die Karte sperren.
8. Verwahren Sie die Smartcard sorgfältig und schützen Sie sie vor Beschädigung und Zerstörung.
9. Verwenden Sie Ihre Smartcard nur auf vertrauenswürdigen Systemen der Bundesverwaltung, für die zugelassenen Applikationen und für den vorgesehenen Zweck.
10. Auf Auslandsreisen dürfen Sie die Smartcard nur dann mitnehmen, wenn Sie diese auch wirklich benötigen.
11. Sie dürfen keine Eingriffe in die Hard- oder Software der Smartcard vornehmen oder vornehmen lassen.

Kontaktstelle:

Haupt RA
Loge VZ VBS
Papiermühlestrasse 20
3003 Bern
Telefon: +41 58 464 64 67